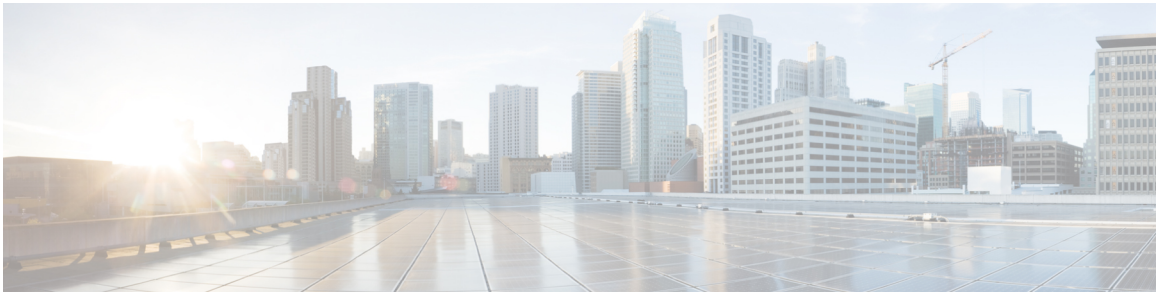


Cisco Catalyst IW9167E Heavy Duty Access Point Configuration Guide, Release 17.16.x

First Published: 2024-12-11

Last Modified: 2025-07-17

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

CHAPTER 1 **Introduction** 1

Overview of the Access Point 1

Determine Image on IW9167EH 2

Configuring AP to Boot up with Different Image Options 3

Upgrade IW9167EH with 17.9.x to Support WGB/uWGB 3

Related Documentation 4

CHAPTER 2 **AP Mode Configuration** 7

Configuring Indoor Deployment for -E Domain 7

802.11ax 1600ns and 3200ns Guard Interval Support 10

Configuring 802.11ax Long Guard Interval 10

GNSS Support 11

RAP Ethernet Daisy Chain 12

WSTP Overview 13

Comparison with Previous Release 13

RAP Ethernet Daisy Chain Configuration 14

Preconfiguring RAP Ethernet Daisy Chain Before Field Deployment 14

Enabling RAP Ethernet Daisy Chain 16

Configuring Super Root 17

Configuring Primary Ethernet Port 18

Configuring Ethernet Bridging and Ethernet Port 18

Show and Debug Command 21

CHAPTER 3 **Workgroup Bridges** 23

Overview 24

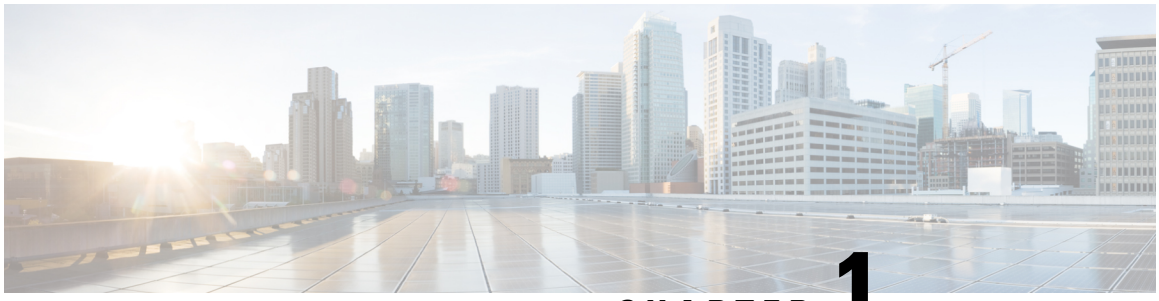
Limitations and Restrictions 24
Configuring Strong Password in Day0 25
Controller Configuration for WGB 27
uWGB Image Upgrade 27
WGB Configuration 28
Configure IP address 29
Configure IPv4 address 29
Configure IPv6 address 30
Configure a Dot1X credential 30
Deauthenticate WGB wired client 31
Configure an EAP profile 31
Configure trustpoint manual enrollment for terminal 32
Configure trustpoint auto-enrollment for WGB 33
Configure manual certificate enrollment using TFTP server 34
SSID configuration 35
Create an SSID profile 35
Configuring Radio Interface for Workgroup Bridges 36
Configuring WGB/uWGB Timer 37
uWGB Configuration 37
Configure IP address 38
Configure IPv4 address 38
Configure IPv6 address 38
Configure a Dot1X credential 39
Configure an EAP profile 39
Configure trustpoint manual enrollment for terminal 40
Configure trustpoint auto-enrollment for WGB 41
Configure manual certificate enrollment using TFTP server 42
SSID configuration 43
Create an SSID profile 43
Configuring Radio Interface for uWGB 44
Converting Between WGB and uWGB 45
LED Pattern 45
Configuring HT Speed Limit 46
Radio Statistics Commands 47

Syslog 50
Event Logging 50
802.11v features 51
Configure Aux Scanning 52
Scan-only mode 52
Scanning only mode 53
Radio 4 as Scanning-Only Mode 54
Configuring Aux-Scan Handoff Mode 56
Optimized Roaming with Dual-Radio WGB 58
Layer 2 NAT 58
Configuration Example of Host IP Address Translation 59
Configuration Example of Network Address Translation 61
Native VLAN on Ethernet Ports 61
Low latency profile 62
Configuring WGB optimized-video EDCA Profile 62
Configuring WGB optimized-automation EDCA Profile 62
Configuring WGB customized-wmm EDCA profile 63
Configuring Low Latency Profile on WGB 63
Configure EDCA parameters using Controller GUI 64
Configuring EDCA Parameters (Wireless Controller CLI) 65
Configuring A-MPDU 66
Configuring WGB/uWGB Radio Parameters 66
Configuring WGB Radio Antenna 66
802.11ax 1600ns and 3200ns Guard Interval 67
Customized Transmit Power 67
Assign Country Code to WGB/uWGB With -ROW PID 67
Indoor Deployment for -E Domain and United Kingdom 67
Configuring WGB Roaming Parameters 68
Importing and Exporting WGB Configuration 68
Verifying the Configuration of WGB and uWGB 69
SNMP features 71
Supported SNMP MIB files 72
Configure SNMP parameters 72
Verifying SNMP 73

QoS ACL classification and marking 73
Rule-based traffic classifications 74
QoS and ACL traffic classification methods 75
Configure QoS Mapping Profile 77
Verify Quality of Service Map 78
Packet Capture: TCP Dump on WGB 79
Packet Capture: TCP dump utilities 79
Enable Wired Packet Capture on WGB 81
Disable wired packet captures 84
Verify wired packet capture 84
AAA User Authentication Support 85
AAA user authentications 85
Configure AAA Server 86
Enable or disable RADIUS authentication for login user 87
Enable or disable TACACS+ authentication for login user 87
AAA authentication configuration example 88
Port Address Translation 89
Port address translations 89
NAPT rules and mapping tables 91
Upstream and downstream data flows 91
Configure NAPT on WGB 93
Delete NAPT mapping rule 94
Delete NAPT IP address 95
Verify NAPT on WGB 95
Port Address Translation on uWGB 96
Port Address Translation 96
NAPT rule and mapping table 97
Upstream and downstream data flow 98
Configure NAPT on uWGB 98
Delete NAPT mapping rule 100
Delete NAPT IP address 101
Manage uWGB in NAPT deployment 101
Verify NAPT on uWGB 102
10 Mbps Speed Port Support on Cisco IW9167EH WGB 104

10 Mbps speed negotiation on Ethernet port 104
Enable 10 Mbps speed port on Cisco IW9167EH WGB 104
Disable 10 Mbps speed port on Cisco IW9167EH WGB 105

CHAPTER 4 **Automated Frequency Coordination** 107
AFC Support for 6 GHz Standard Power Mode 107
Verifying AFC Status on AP 108



CHAPTER 1

Introduction

- Overview of the Access Point, on page 1
- Determine Image on IW9167EH, on page 2
- Configuring AP to Boot up with Different Image Options, on page 3
- Upgrade IW9167EH with 17.9.x to Support WGB/uWGB, on page 3
- Related Documentation, on page 4

Overview of the Access Point

The Cisco Catalyst IW9167E Heavy Duty Access Point provides reliable wireless connectivity for mission-critical applications in a state-of-the art platform. It can operate as Cisco Catalyst Wi-Fi (CAPWAP) mode or Cisco Ultra-Reliable Wireless Backhaul (Cisco URWB) mode starting from IOS XE Cupertino 17.9.3 Software Release. The IW9167EH access point has the flexibility to change the operating mode from Wi-Fi to Cisco URWB, and vice versa.

Starting from Cisco IOS XE Dublin 17.11.1, Workgroup Bridge (WGB) and Universal WGB (uWGB) are supported on the Cisco Catalyst IW9167E Heavy Duty Access Points.

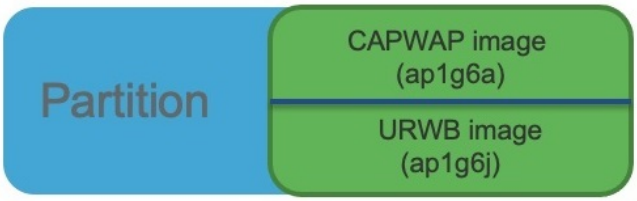
This document covers configuration of CAPWAP mode and WGB/uWGB mode specific to the IW9167EH access points.

For CAPWAP mode, the access points can operate in the following modes:

- Local
- Flexconnect
- Bridge
- Flexconnect + Bridge
- Sniffer
- Monitor
- Site survey

Determine Image on IW9167EH

Software images are stored under different folders on the same partition on IW9167EH.



You need to choose the image to boot up with according to the mode your AP is runnning, CAPWAP, Cisco URWB, or WGB/uWGB. The following table provides the software images of each mode:

Table 1: IW9167EH Software Images

IW9167EH Mode	Software Image
CAPWAP	**ap1g6a-k9w8-xxx.tar**
Cisco URWB	Unified Industrial Wireless image **ap1g6j-k9c1-xxx.tar**
WGB/uWGB	

To determine the image that your IW9167EH is running, use the **show version** command.

- If the **show version** output displays **Cisco AP Software, (ap1g6a)** as shown in the following example, it means that AP is running the CAPWAP image **ap1g6a-k9w8-xxx.tar**, which supports the CAPWAP mode.

```
Cisco AP Software, (ap1g6a), C9167, RELEASE SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2022 by Cisco Systems, Inc.
Compiled Fri Jul 29 01:56:00 PDT 2022

ROM: Bootstrap program is U-Boot boot loader
BOOTLDR: U-Boot boot loader Version 2022010100

APFC58.9A16.E648 uptime is 0 days, 1 hours, 03 minutes
Last reload time   : Mon Sep 19 02:23:13 UTC 2022
Last reload reason : Image Upgrade

cisco IW9167EH-B ARMv8 Processor rev 4 (v8l) with 1757076/1006864K bytes of memory.
```

- If the **show version** output displays **Cisco AP Software (ap1g6j)** as shown in the following example, it means that AP is running **ap1g6j-k9c1-xxx.tar** image, which supports the Cisco URWB mode or Cisco WGB/uWGB.

```
Cisco AP Software, (ap1g6j), C9167, RELEASE SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2022 by Cisco Systems, Inc.
Compiled Thu Aug 18 01:01:29 PDT 2022

ROM: Bootstrap program is U-Boot boot loader
BOOTLDR: U-Boot boot loader Version 2022010100

APFC58.9A16.E464 uptime is 1 days, 3 hours, 58 minutes
```

```
Last reload time   : Wed Sep 7 11:17:00 UTC 2022
Last reload reason : reload command

cisco IW9167EH-B ARMv8 Processor rev 4 (v8l) with 1759128/1091316K bytes of memory.
```

Configuring AP to Boot up with Different Image Options

To configure the access point to boot up with CAPWAP, URWB, or WGB/uWGB mode, follow these steps:

Note Switching between different modes performs full factory reset. Any configuration and data will be removed completely.

Procedure

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

Step 2 **configure boot mode** {**capwap** | **urwb** | **wgb**}

Configures AP to CAPWAP, URWB, or WGB/uWGB mode. AP will reboot with specified mode.

Upgrade IW9167EH with 17.9.x to Support WGB/uWGB

If your IW9167EH is shipped with Cisco IOS XE Cupertino 17.9.3 software and operating as CAPWAP mode, and you want to upgrade your AP to Cisco IOS XE Dublin 17.11.1 to support WGB/uWGB mode, you need to switch your AP to Cisco URWB mode first, and then you can upgrade to 17.11.1.

To determine whether your IW9167EH is running CAPWAP mode or Cisco URWB mode, use the **show version** command.

- If the **show version** output displays **Cisco AP Software (ap1g6a)**, your AP is running as CAPWAP mode.
- If the **show version** output displays **Cisco AP Software (ap1g6j)**, your AP is running as Cisco URWB mode.

Cisco WGB/uWGB mode shares the same image with Cisco URWB. You cannot upgrade the **ap1g6j** image to 17.11.1 in CAPWAP mode (**ap1g6a**). Because the **archive download** command checks image type, upgrade gets aborted if image types mismatch.

Procedure

Step 1 Convert CAPWAP mode to Cisco URWB mode.

Example:

```
#configure boot mode urwb
       Before image swapping device need factory reset. Are you sure to proceed? (Y/N):y
       Converting to Cisco URWB Mode...
       <rebooting…>
```

Step 2 Log in with default credential (Cisco/Cisco/Cisco).

Step 3 Configure Cisco URWB, to make it work in **Offline** mode.

Example:

```
#configure iotod-iw offline
       Switching to IOTOD IW Offline mode...
       Will switch from Provisioning Mode to IOTOD IW offline Mode, device need to reboot: Y/N?  Y
       <rebooting…>
```

Step 4 Configure networking in Cisco URWB (IP/netmask/gateway, passphrase)

Example:

```
Cisco-23.174.76#configure wireless passphrase unit1
Cisco-23.174.76#configure ap address ipv4 static 192.168.1.200 255.255.255.0 192.168.1.1
Cisco-23.174.76#write
Cisco-23.174.76#reload
     <rebooting…>
```

Note
Passphrase is optional, but it is recommended to assign different passphrases if you are upgrading multiple units at the same time and they are connected to the same Layer 2 network. Because Cisco URWB forms MPLS network automatically if all nodes have the same passphrase, without further MPLS configuration, your IP service might not work properly.

Step 5 Upgrade to 17.11.1.

Example:

```
#archive download-sw /reload tftp://<TFTP_SERVER>/<ap1g6j-FILENAME>
          <rebooting…>
```

Step 6 Convert the AP from Cisco URWB mode to Cisco WGB/uWGB mode.

Example:

```
#configure boot mode wgb
           <rebooting…>
```

Related Documentation

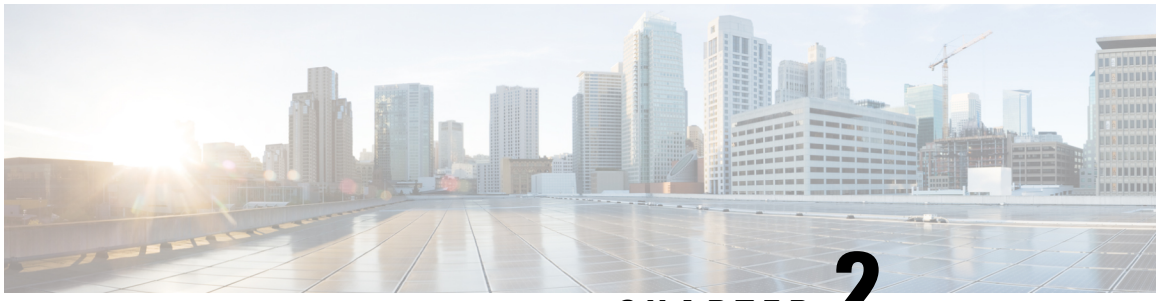
To view all support information for the Cisco Catalyst IW9167E Heavy Duty Access Point, see https://www.cisco.com/c/en/us/support/wireless/catalyst-iw9167-series/series.html.

In addition to the documentation available on the support page, you will need to refer to the following guides:

- For information about IW9167EH hardware, see Cisco Catalyst IW9167E Heavy Duty Access Point Hardware Installation Guide.
- A full listing of the AP's features and specifications is provided in Cisco Catalyst IW9167E Heavy Duty Access Point Data Sheet.
- For more information about the configuration on Cisco Catalyst 9800 Series Wireless Controllers, see https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-installation-and-configuration-guides-list.html.
- For information about Cisco URWB mode configuration, see the relevant documents at:

  https://www.cisco.com/c/en/us/support/wireless/catalyst-iw9167-series/series.html.
- For more information about Cisco IOS XE, see the relevant documents at:

  http://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-xe/index.html



CHAPTER 2

AP Mode Configuration

- Configuring Indoor Deployment for -E Domain, on page 7
- 802.11ax 1600ns and 3200ns Guard Interval Support, on page 10
- GNSS Support, on page 11
- RAP Ethernet Daisy Chain, on page 12

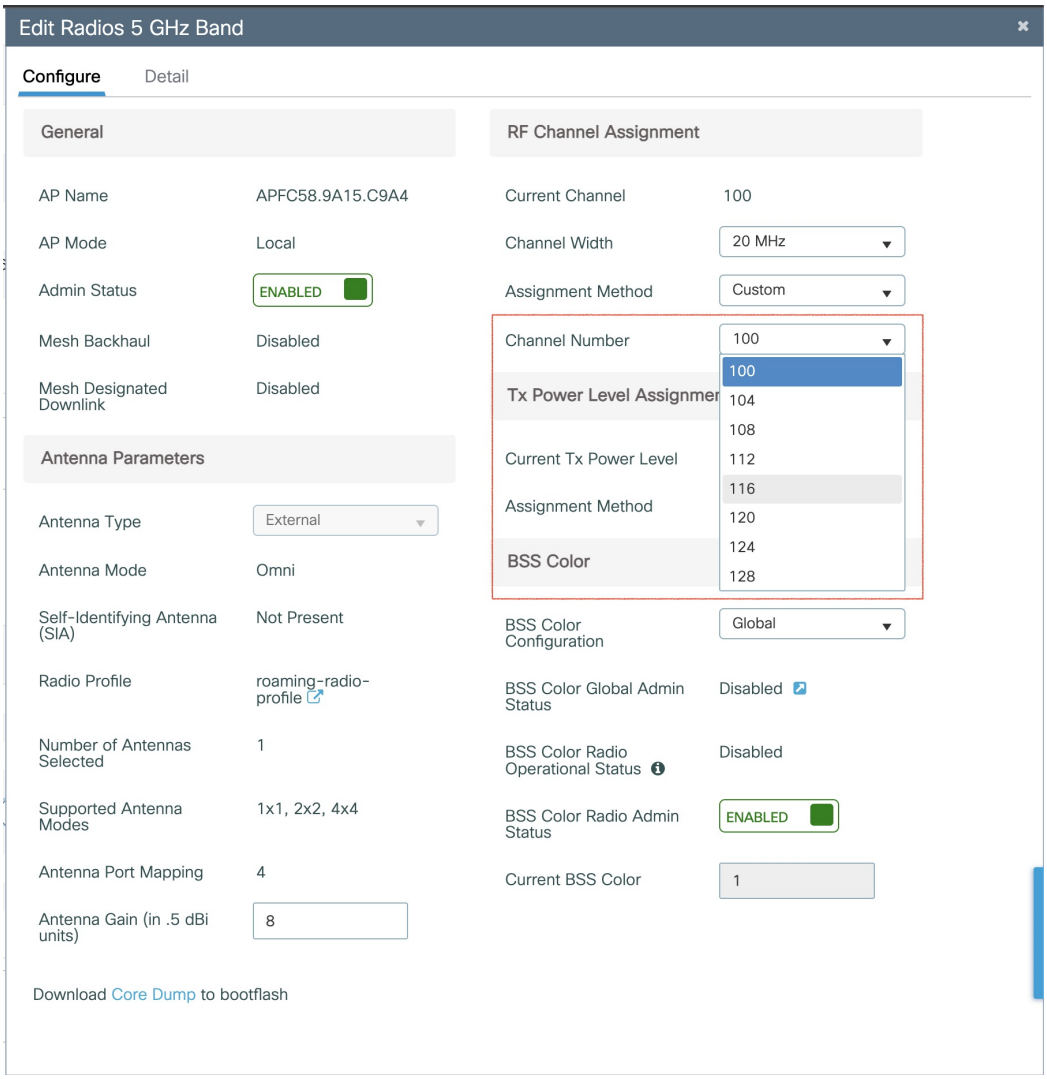
Configuring Indoor Deployment for -E Domain

IW9167EH supports indoor deployment for -E domain.

By default, indoor deployment is disabled, and the 5G radio supports channels 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140. After factory reset, indoor deployment configuration is reset to default, which is disabled.

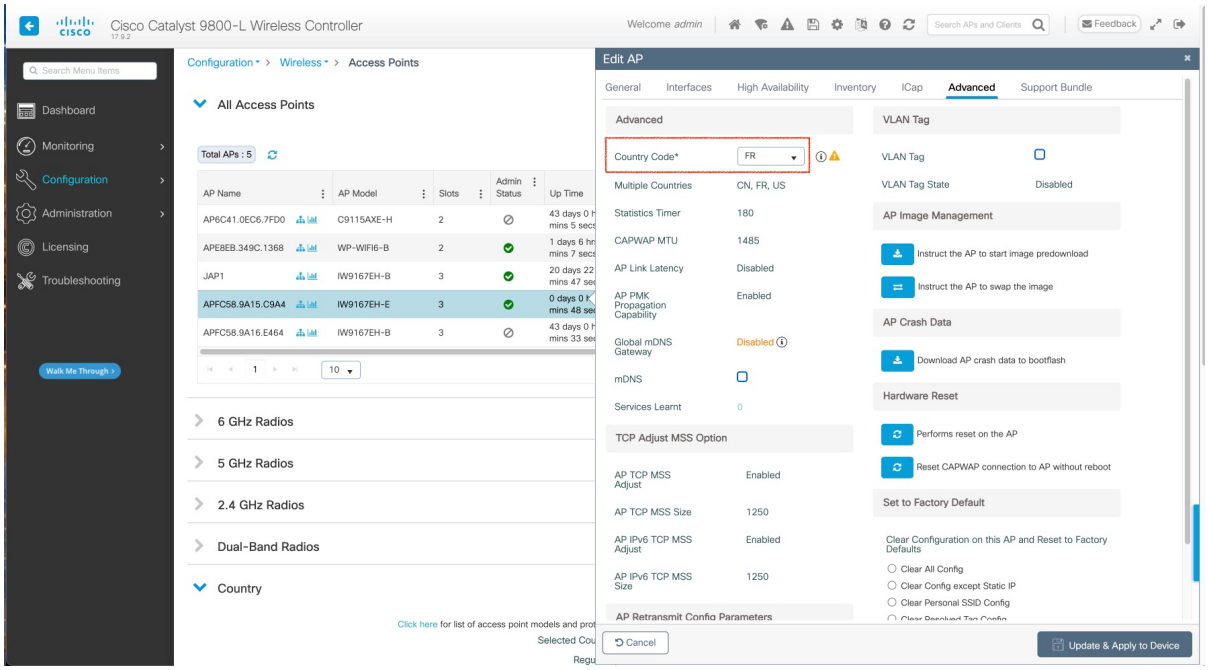
You can check AP mode by using the **show ap name <ap-name> config general | section Indoor** command. In the command output, "Enabled" means AP is in indoor mode, and "Disabled" means AP is in outdoor mode, as shown in the following example.

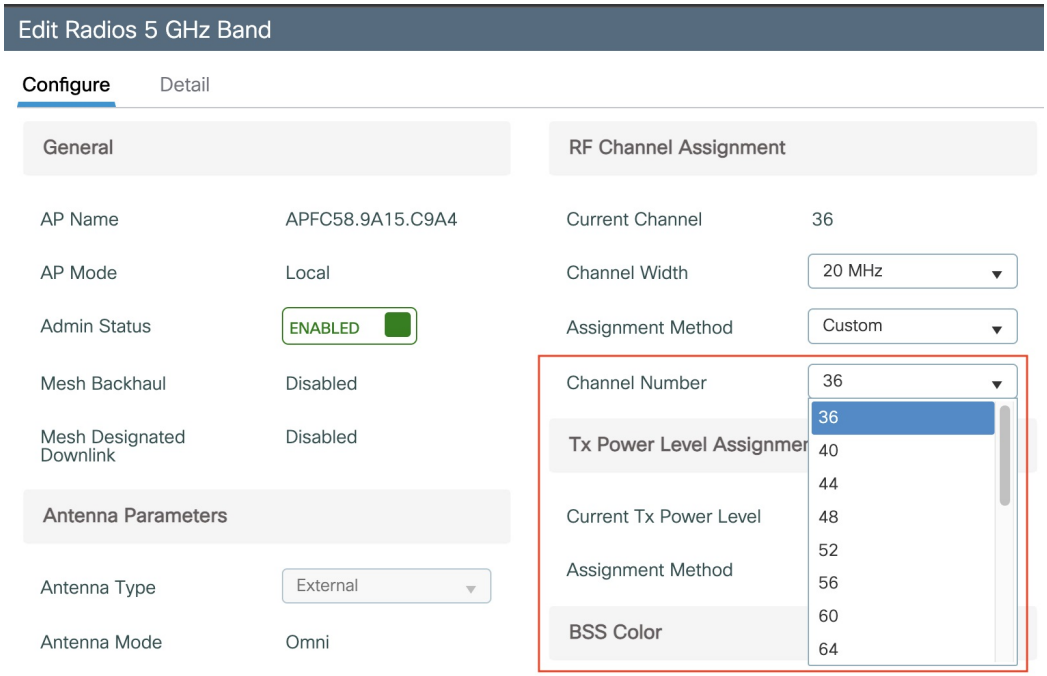
```
#show ap name APFC58.9A15.C9A4 config general | inc Indoor
    AP Indoor Mode                                  : Disabled
```



To configure the AP to indoor mode, use the **ap name** <*ap-name*> **indoor** command from wireless LAN controller. This command triggers an AP rebooting. After AP registers to the wireless LAN controller after rebooting, you need to assign corresponding country code to the AP. When indoor deployment is enabled, 5G radio supports channels 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140.

Note To disable indoor deployment, use the **ap name** <*ap-name*> **no indoor** command.





Note Channel list extends from U-NII-2c to U-NII-1, U-NII-2a, U-NII-2c (channel 144 is excluded).

802.11ax 1600ns and 3200ns Guard Interval Support

802.11ac has two Guard Interval (GI) options – long GI (800ns) and short GI (400ns). 802.11ax introduces new guard interval options. It has three types of GI – 800ns, 1600ns, and 3200ns. Longer guard intervals provide improved performance in environments with multi-path and delay spread. It improves link reliability for longer-range outdoor deployments and helps to prevent inter-symbol interference in outdoor environments and therefore improve coverage and performance.

The following table compares 802.11ax to the previous two standards.

Table 2: 802.11ax Guard Interval Comparing With Previous Standards

Capabilities	802.11n	802.11ac	802.11ax
Physical Layer (PHY)	High Throughput (HT)	Very High Throughput (VHT)	High-Efficiency (HE)
Guard Interval	800/400 ns	800/400 ns	800/1600/3200 ns

Configuring 802.11ax Long Guard Interval

HE mode guard intervals should be configured in RF profiles.

Procedure

Step 1 Enters global configuration mode.

```
Device#configure terminal
```

Example:

```
Device#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

Step 2 Configures RF profile and enters RF profile configuration mode

ap dot11 {**24ghz**|**5ghz**} **rf-profile** *<profile-name>*

Example:

```
Device(config)#ap dot11 24ghz rf-profile 24G-RF-profile
```

Step 3 Configures guard interval for the RF profile.

guard-interval {**GUARD_INTERVAL_1600NS** | **GUARD_INTERVAL_3200NS** | **GUARD_INTERVAL_400NS** | **GUARD_INTERVAL_800NS**}

Example:

```
Device(config-rf-profile)#guard-interval GUARD_INTERVAL_1600NS
```

- GUARD_INTERVAL_1600NS: Set 1600 ns guard interval (only in HE mode)
- GUARD_INTERVAL_3200NS: Set 3200 ns guard interval (only in HE mode)

- GUARD_INTERVAL_400NS: Set 400 ns guard interval (HT VHT mode)
- GUARD_INTERVAL_800NS: Set 800 ns guard interval

Note
Valid guard interval values are 800, 1600, and 3200 ns for HE mode. By default, GI is 800 ns.

Step 4 Exit global configuration mode.

end

Example:

```
Device(config)#end
```

Use the following command to verify the configuration on wireless controller:

```
#show ap rf-profile name Demo-24G-RF-profile detail | inc Guard
Guard Interval        : 1600ns
#show ap rf-profile name Demo-5G-RF-profile detail | inc Guard
Guard Interval        : 3200ns
```

Example

1. Define GI in RF profile

```
ap dot11 24ghz rf-profile Demo-24G-RF-profile
shutdown
guard-interval GUARD_INTERVAL_1600NS
no shutdown
ap dot11 5ghz rf-profile Demo-5G-RF-profile
shutdown
guard-interval GUARD_INTERVAL_3200NS
no shutdown
```

2. Associate RF profile to RF tag

```
wireless tag rf Demo-Guard-Interval-RF-tag
24ghz-rf-policy Demo-24G-RF-profile
5ghz-rf-policy Demo-5G-RF-profile
```

3. Associate RF tag to AP

```
ap fc58.9a15.c83c
rf-tag Demo-Guard-Interval-RF-tag
```

GNSS Support

From Cisco IOS XE Dublin 17.11.1, GNSS is supported on IW9167EH. The AP tracks GPS information for devices deployed in the outdoor environment and sends the GNSS information to the wireless controller.

Use the following command to display the GNSS information on the AP:

ap# **show gnss info**.

Use the following commands to display the GPS location of the AP:

controller# **show ap geolocation summary**

controller# **show ap name** <*Cisco AP*> **geolocation detail**

RAP Ethernet Daisy Chain

The RAP Ethernet Daisy Chain feature enhances the existing Ethernet bridging functionality. It forces the bridge AP to stick to the Ethernet link, and block the selecting of wireless link for uplink backhaul. Even the Ethernet link failure happens, the access point will never select a parent over wireless backhaul.

The following figure shows an example of RAP Ethernet Daisy Chain topology. Standalone DC power source is provided to each RAP.

Figure 1: RAP Ethernet Daisy Chain Topology

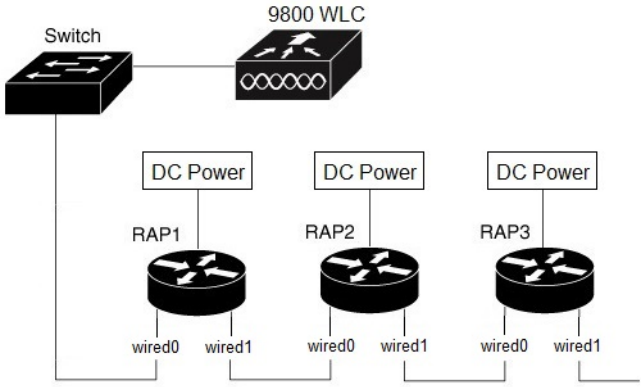


Table 3: Port Mapping

Panel Label	SW Interface
mGig POE-IN port	wired 0
SFP	wired 1

Note The supported SFP module for this feature is the 1000BASE-T rugged SFP (Cisco PID: GLC-T-RGD).

Follow these guidelines when you configure this feature:

- All APs in daisy chain is operating in mesh bridge mode or Flex+Bridge mode with Root AP role. The PoE-IN (wired0) and SFP (wired1) port can be used as uplink port and the PoE-IN (wired0) port has the higher priority than SFP (wired1).
- VLAN transparency should be disabled on all daisy-chained RAPs.
- To enable VLAN support on each root AP:
  - For bridge mode APs, use the **ap name name-of-rap mesh vlan-trunking [native] vlan-id** command to configure a trunk VLAN on the corresponding RAP.
  - For Flex+Bridge APs, you must configure the native VLAN ID under the corresponding flex profile.

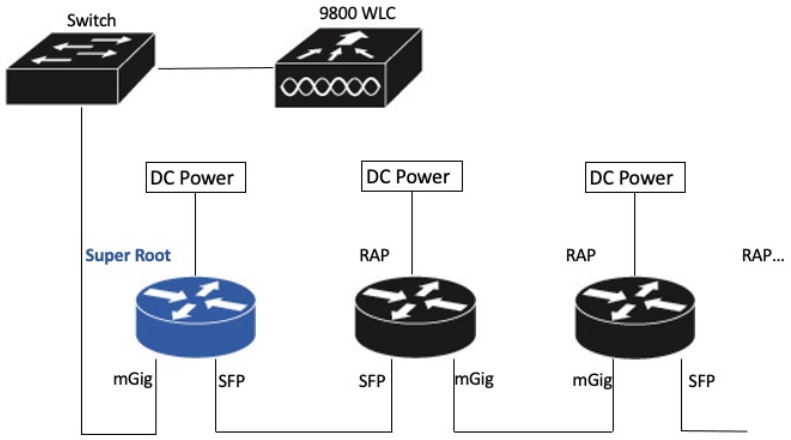
The RAP Ethernet Daisy Chain feature is already supported on Cisco IOS XE Cupertino 17.9.3, while it has the following limitations:

- Primary ethernet port (mGig port) must be used as uplink. In this case, SFP port to SFP port connection is not supported, which impacts network throughput (no 2.5Gbps or 5Gbps copper SFP available when SFP connect to mGig port).
- Reuse an existing command **persistant-ssid** to enable the RAP Ethernet Daisy Chain feature, which is misleading.

In Cisco IOS XE Dublin 17.11.1, the RAP Ethernet Daisy Chain feature is enhanced to support the following functions:

- Wireless Spanning Tree Protocol (WSTP) hello is enabled to support auto root port detection, so that RAP can use any port as its uplink. See the following topology.

Figure 2: RAP Ethernet Daisy Chain With WSTP Topology



- A separate and dedicated command **rap-eth-daisychain** is introduced to enable the feature.

WSTP Overview

Wireless LAN spanning tree protocol (WSTP) organizes a Cisco mesh network into a loop-free spanning tree topology. It quickly configure a mesh network into a stable, loop-free, optimal spanning tree topology, where an optimal topology provides least-cost paths to the primary Ethernet LAN. WSTP Hello messages are used to build the WSTP topology.

The WSTP super root is a single RAP that is elected as the highest level “super” root for the entire WSTP spanning tree. The super root is directly attached to the primary LAN. The super root transmits zero-cost WSTP SR Hello messages on its Ethernet root port to advertise the primary LAN to RAPs.

Comparison with Previous Release

The following table compares the daisy chain features in current release and prior to 17.11:

	Prior to Release 17.11.1	Release 17.11.1
Topology	**Fixed topology** RAP must use its mGig port as uplink in daisy chain topology	**Flexible topology** RAP can use either mGig port or SFP port as uplink in daisy chain topology by enabling WSTP on AP
Feature enablement	**Persistant-ssid** in AP profile [1]	**rap-eth-daisychain** in Mesh profile
Ring Topology	Not supported [2]	Not supported

[1] **Persistant-ssid** is still supported in 17.11, so that daisy chain function will not be impacted after upgrading from previous release to 17.11 with old configuration. But **Persistant-ssid** is not recommended in 17.11, and the new **rap-eth-daisychain** command is recommended.

[2] Supported only on IW6300 access point, by enabling **daisychain-stp-redundancy**. For more information, see the RAP Ethernet Daisy Chain Redundancy for STP Ring Topology section in Cisco Catalyst IW6300 Heavy Duty Series and 6300 Series Embedded Services Access Point Software Configuration Guide.

RAP Ethernet Daisy Chain Configuration

This section provides procedures for the RAP Ethernet daisy chain configuration.

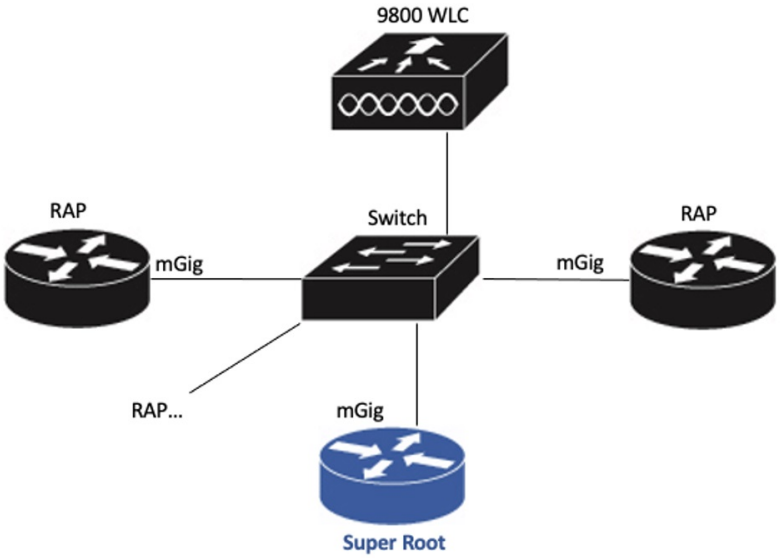
Preconfiguring RAP Ethernet Daisy Chain Before Field Deployment

This section provides the preconfiguration that you should complete in lab before you set up in field deployment.

Procedure

Step 1 Unpack, connect, and power on the AP.

Step 2 Join each AP to controller with mGig port. See the following figure for details.



Step 3 Configure AP to bridge mode and configure AP role to Root AP.

For detailed configuration procedures, see https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-11/config-guide/b_wl_17_eleven_cg/m_mesh_ewlc.html#task_pnb_bwy_mlb.

Step 4 Configuring RAP Ethernet Daisy Chain.

a) Create mesh profile and enable the Rap Ethernet Daisy chain feature.

See Enabling RAP Ethernet Daisy Chain, on page 16.

b) Attach the profile to all the RAP.

c) Configure one AP as Super Root which should be the first hop to the wireless controller.

See Configuring Super Root, on page 17.

d) Configure primary Ethernet port on the Super Root AP if you use SFP port as uplink.

See Configuring Primary Ethernet Port, on page 18.

Step 5 Enable Ethernet Bridging and Configure Ethernet port.

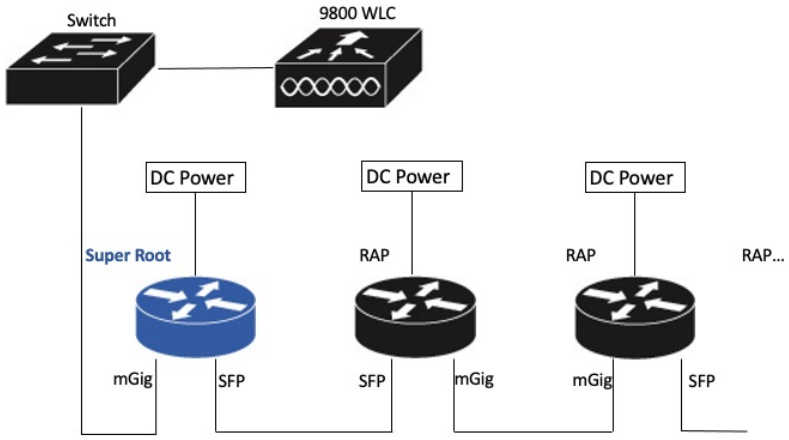
See Configuring Ethernet Bridging and Ethernet Port, on page 18.

a) Enable Ethernet Bridging.

b) Ethernet port configuration on both Port 0 and Port 1, including port mode and vlan. It is recommended to configure port to trunk mode.

Step 6 Verify the behavior in daisy chain topology.

a) Connecting the RAP via wired port one by one.



Note
The RAP which is the first hop from wireless controller should be configured as Super Root, as shown in the above figure.

b) Make sure that RAP of each hop can join the controller.

Note
In field deployment, just repeat Step 6 of this procedure. Make sure you configure the first hop as Super Root.

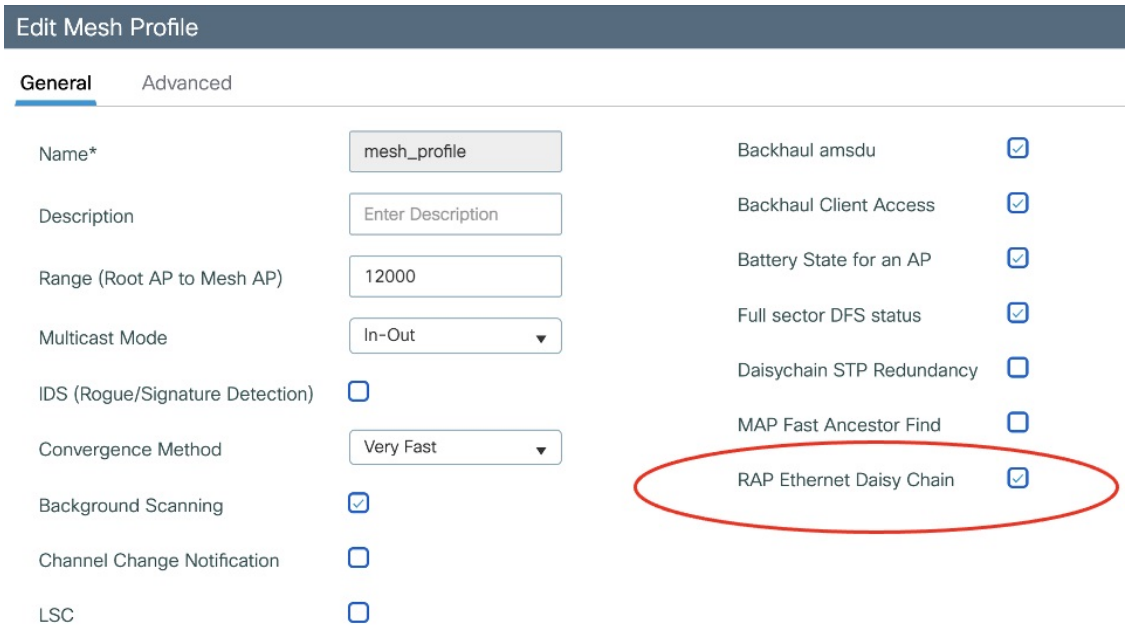
Enabling RAP Ethernet Daisy Chain

To enable RAP Ethernet Daisy Chain feature, use the **rap-eth-daisychain** command, or configure from GUI.

The following example shows enabling the feature from CLI:

```
#configure terminal
(config)#wireless profile mesh default-mesh-profile
(config-wireless-mesh-profile)#ethernet-bridging
(config-wireless-mesh-profile)#rap-ethernet-daisychain
```

The following figure shows enabling the feature from GUI:



To verify the configuration, use the **show wireless profile mesh detailed** command or **show wireless mesh ethernet daisy-chain summary** command from wireless controller, as shown in the following examples:

```
#show wireless profile mesh detailed <profile name>
…
RAP ethernet daisychain       : ENABLED

#show wireless mesh ethernet daisy-chain summary
AP Name      BVI MAC        BGN        Backhaul          Ethernet      STP Red        Super
 Root
-----------------------------------------------------------------------------------------------
APxxxxxx     xxxxxxx       xxxxx       Ethernet0          Up Up          NA
Enabled
```

Or use the **show mesh config** command on AP, as shown in the following example:

```
#show mesh config
…
RAP Ethernet Daisy Chain: Enabled
  Daisy Chain Root: Disabled
```

Configuring Super Root

The first RAP which connects to the upstream switch should be configured as super root, which means it's the source of all WSTP hello. Other RAPs only start hello after receiving a hello.

You can configure the super root from wireless controller or from AP.

- From wireless controller, use the **ap name <name> [no] mesh rap-eth-daisychain super-root** command to configure a super root.

  To verify the configuration, use the following command:

  ```
  #show ap name <name> config general
  …
  RAP ethernet daisychain                : Enabled
  Super Root                             : Enabled
  ```

- On AP, use the **capwap ap mesh wstp super-root** command to configure a super root.

  To verify the configuration, use the following command:

```
#show mesh config
…
RAP Ethernet Daisy Chain: Enabled
  Daisy Chain Root: Enabled
```

Configuring Primary Ethernet Port

Super root must use its primary Ethernet port to connect to upstream switch. For IW9167EH, the default primary Ethernet port is Ethernet port 0. To manually configure the primary Ethernet port, use the **ap name <name> mesh backhaul ethernet <0/1>** command from wireless controller.

To verify the configuration, use the following command from wireless controller:

```
#show ap name <name> config general
…
AP Primary Ethernet port                        : 1
RAP ethernet daisychain                         : Enabled
Super Root                                      : Disabled
```

Or use the following commands on AP:

```
#show mesh config
…
RAP Ethernet Daisy Chain: Enabled
  Daisy Chain Root: Enabled
AP Primary ethernet backhaul interface: 1

#show mesh adjacency parent
AdjInfo: Wired Backhaul: 1 [xx:xx:xx:xx:xx:xx]
```

Configuring Ethernet Bridging and Ethernet Port

Configuring Ethernet Bridging (CLI)

The Ethernet port on the MAPs are disabled by default. It can be enabled only by configuring Ethernet bridging on the Root AP and the other respective MAPs. Follow these steps to enable Ethernet bridging on the AP.

Procedure

Step 1 Enters global configuration mode.

```
Device#configure terminal
```

Step 2 Creates a mesh profile.

wireless profile mesh *profile-name*

Example:

```
(config)#wireless profile mesh rap-eth-daisy
```

Step 3 **ethernet-bridging**

Example:

```
(config-wireless-mesh-profile)#ethernet-bridging
```

Connects remote wired networks to each other.

Step 4 Disables VLAN transparency to ensure that the bridge is VLAN aware.

no ethernet-vlan-transparent

Example:

```
(config-wireless-mesh-profile)#no ethernet-vlan-transparent
```

Step 5 Exit global configuration mode.

end

Example:

```
(config-wireless-mesh-profile)#end
```

Example

Use the following command to verify the configuration:

```
#show wireless profile mesh detailed rap-eth-daisy

Mesh Profile Name           : rap-eth-daisy
-------------------------------------
Description                 :
Bridge Group Name           : unconfigured
Strict match BGN            : DISABLED
Amsdu                       : ENABLED
Background Scan             : DISABLED
Channel Change Notification : DISABLED
Backhaul client access      : DISABLED
Ethernet Bridging           : ENABLED
Ethernet Vlan Transparent   : DISABLED
Daisy Chain SP Redundancy   : DISABLED
Full Sector DFS             : ENABLED
```

Configuring Ethernet Bridging (GUI)

Follow these steps to configure Ethernet Bridging from wireless controller GUI:

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Mesh** > **Profiles**

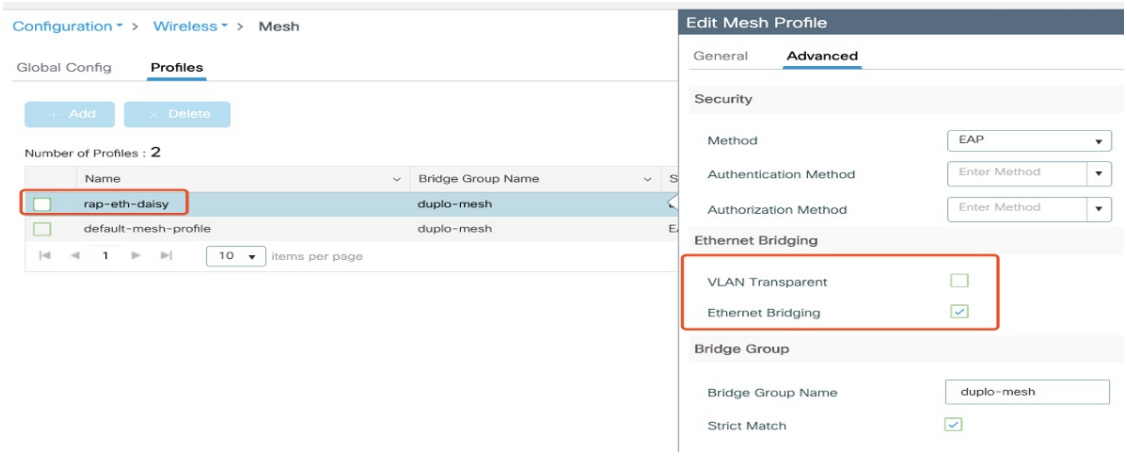
Step 2 Click **Add**.

Step 3 In **General** tab, enter the **Name** of the mesh profile.

Step 4 In **Advanced** tab, uncheck the **VLAN Transparent** check box to disable VLAN transparency.

Step 5 In **Advanced** tab, check the **Ethernet Bridging** check box.

Step 6 Click **Apply to Device**.



Configuring Ethernet Port (CLI)

RAP Ethernet secondary port supports Access mode and Trunk mode. Follow these steps to configure Ethernet port mode.

- Use the following command to configure access mode.

  #**ap name** *ap-name* **mesh ethernet 1 mode access** *Vlan-ID*

- Use the following commands to configure trunk mode. VLAN support must be enabled in advance, and VLAN transparent should be disabled in your mesh profile.
  - Configure a trunk VLAN on the corresponding RAP.

    #**ap name** *ap-name* **mesh vlan-trunking native** *Vlan-ID*

  - Configure the native VLAN for the trunk port.

    #**ap name** *ap-name* **mesh ethernet 1 mode trunk vlan native** *Vlan-ID*

  - Configure the allowed VLANs for the trunk port. Permits VLAN filtering on an ethernet port of any Mesh or Root Access Point. Active only when VLAN transparency is disabled in the mesh profile.

    #**ap name** *ap-name* **mesh ethernet 1 mode trunk allowed** *Vlan-ID*

Configuring Ethernet Port (GUI)

Follow these steps to configure Ethernet port from wireless controller GUI:

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

The **All Access Points** section, which lists all the configured APs in the network, is displayed with their corresponding details.

Step 2 Click the configured mesh AP.

The **Edit AP** window is displayed.

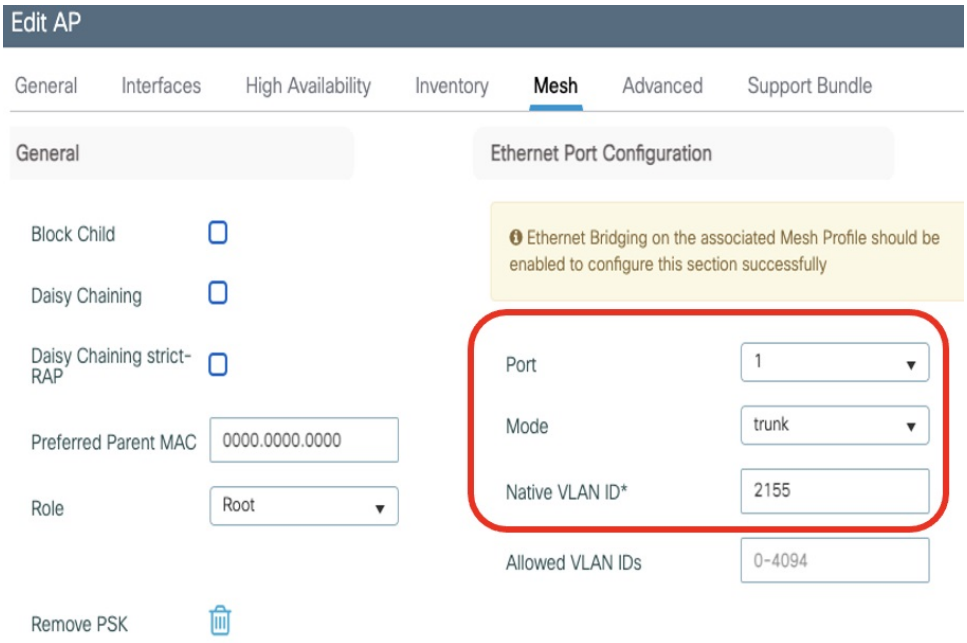
Step 3 Choose the **Mesh** tab.

Step 4 In the **Ethernet Port Configuration** section, from the **Port** drop-down list, choose the port to configure.

Step 5 From the **Mode** drop-down list, choose access mode or trunk mode.

Step 6 In the **Native VLAN ID** field, enter the native VLAN for the trunk port.

Step 7 Click **Update and Apply to Device**.



Show and Debug Command

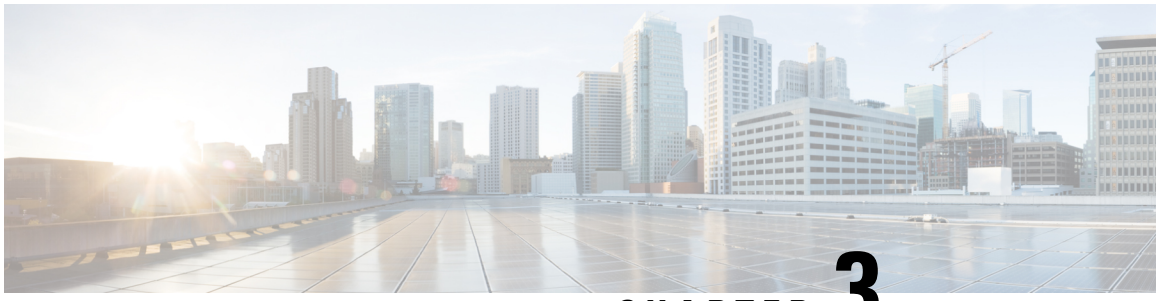
- Use the following command to debug WTP:

```
AP#debug mesh wstp
  error     Mesh wstp error debugs
  events    Mesh wstp events debugs
  packets   Mesh wstp packet debugs
```

```
03:05:24.5918] chatter: wstp_ctl :: WstpControl: RX Hello(00) - BID:FC:58:9A:15:C8:04 SR:FC:58:9A:15:C8:04/0 Flags:02 Port:wired0
03:05:24.5918] chatter: wstp_ctl :: WstpControl - wired_hello_only, hello received, update parent record
03:05:24.5946] chatter: wstp_ctl :: WstpControl: TX Hello(00) - BID:FC:58:9A:17:58:EC SR:FC:58:9A:15:C8:04/0 Flags:02 Port:wired1
03:05:26.5918] chatter: wstp_ctl :: WstpControl: RX Hello(00) - BID:FC:58:9A:15:C8:04 SR:FC:58:9A:15:C8:04/0 Flags:02 Port:wired0
03:05:26.5918] chatter: wstp_ctl :: WstpControl - wired_hello_only, hello received, update parent record
03:05:26.5946] chatter: wstp_ctl :: WstpControl: TX Hello(00) - BID:FC:58:9A:17:58:EC SR:FC:58:9A:15:C8:04/0 Flags:02 Port:wired1
```

- Use the following command to display the WSTP statistics:

```
AP#show mesh stats
WSTP stats:
Attach-Cnt Hello-TX Hello-Rx TCN-TX TCN-RX SR-Chg-Cnt ST-Roam-Cnt
         0       58       58      0      0          0           0
```



CHAPTER 3

Workgroup Bridges

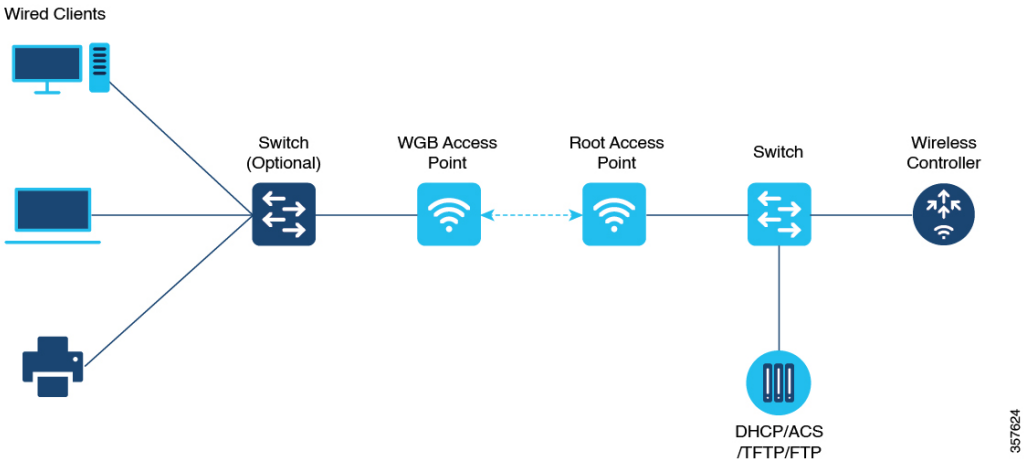
- Overview, on page 24
- Limitations and Restrictions, on page 24
- Configuring Strong Password in Day0, on page 25
- Controller Configuration for WGB, on page 27
- uWGB Image Upgrade, on page 27
- WGB Configuration, on page 28
- uWGB Configuration, on page 37
- Converting Between WGB and uWGB, on page 45
- LED Pattern, on page 45
- Configuring HT Speed Limit, on page 46
- Radio Statistics Commands, on page 47
- Syslog, on page 50
- Event Logging, on page 50
- 802.11v features, on page 51
- Configure Aux Scanning, on page 52
- Layer 2 NAT, on page 58
- Native VLAN on Ethernet Ports, on page 61
- Low latency profile, on page 62
- Configuring WGB/uWGB Radio Parameters, on page 66
- Assign Country Code to WGB/uWGB With -ROW PID, on page 67
- Indoor Deployment for -E Domain and United Kingdom, on page 67
- Configuring WGB Roaming Parameters, on page 68
- Importing and Exporting WGB Configuration, on page 68
- Verifying the Configuration of WGB and uWGB, on page 69
- SNMP features, on page 71
- QoS ACL classification and marking, on page 73
- Packet Capture: TCP Dump on WGB, on page 79
- AAA User Authentication Support, on page 85
- Port Address Translation, on page 89
- Port Address Translation on uWGB, on page 96
- 10 Mbps Speed Port Support on Cisco IW9167EH WGB, on page 104

Overview

A workgroup bridge (WGB) is an Access Point (AP) mode to provide wireless connectivity to wired clients that are connected to the Ethernet port of the WGB AP. A WGB connects a wired network over a single wireless segment by learning the MAC addresses of its wired clients on the Ethernet interface and reporting them to the WLC through infrastructure AP using Internet Access Point Protocol (IAPP) messaging. The WGB establishes a single wireless connection to the root AP, which in turn, treats the WGB as a wireless client.

Universal WGB (uWGB) is a complementary mode of WGB feature that acts as a wireless bridge between the wired client connected to uWGB and wireless infrastructure including Cisco and non-Cisco wireless network. One of the wireless interface is used to connect with the access point. The radio MAC is used to associate AP.

Figure 3: Example of a WGB



Starting from Cisco IOS XE Dublin 17.11.1, WGB is supported on the Cisco Catalyst IW9167E Heavy Duty Access Points.

Limitations and Restrictions

This section provides limitations and restrictions for WGB and uWGB modes.

- The WGB can associate only with Cisco lightweight access points. The universal WGB can associate to a third party access point.
- In a Meraki wireless infrastructure that uses WPA1 security, uWGB do not associate with any SSIDs.
- Speed and duplex are automatically negotiated based on the capabilities of the locally connected endpoint and cannot be manually configured on the AP's wired 0 and wired 1 interfaces.
- The following features are not supported for use with a WGB:
  - Idle timeout
  - Web authentication

- With Layer 3 roaming, if you plug a wired client into the WGB network after the WGB has roamed to another controller (for example, to a foreign controller), the wired client's IP address displays only on the anchor controller, not on the foreign controller.
- When you deauthenticate a WGB record from a controller, all of the WGB wired clients' entries are also deleted.
- These features are not supported for wired clients connected to a WGB:
  - MAC filtering
  - Link tests
  - Idle timeout
- Associating a WGB to a WLAN that is configured for Adaptive 802.11r is not supported.
- WGB supports IPv6 only when IPv4 is enable. But there is no impact on WGB wired clients IPv6 traffic.
- WGB management IPv6 does not work after WGB uplink association is completed. WGB can get an IPv6 address when the association is successful. But IPv6 ping will not be passed from or to WGB. SSH from wireless or wired client to WGB management IPv6 is not working. The workaround to bypass the pingable issue is to re-enable IPv6, even though IPv6 has already been enabled and the IPv6 address has been assigned.
- uWGB mode does not support SSH connecting to itself.
- uWGB mode supports neither TFTP nor SFTP. For software upgrade, you should perform it from WGB mode. For more information, see uWGB Image Upgrade, on page 27.
- uWGB does not support host IP service. Some functions, such as image upgrade via radio uplink and remote management via SSH session, are not supported.
- For IW9167EH WGB/uWGB mode, the **packet retries [N] drop** command does not work in IOS XE Release 17.11.1.
- DFS channels are supported on IW9167EH WGB/uWGB from Release 17.13.1.
- Only Dot11Radio 0 and Dot11Radio 1 interfaces can be used as wireless uplink on IW9167EH WGB/uWGB.
- When the infrastructure AP operates on a non-DFS (Dynamic Frequency Selection) channel and changes its channel bandwidth, the WGB stays connected to the infrastructure AP using the original channel bandwidth.

  To make sure the WGB connects to the AP with the correct channel bandwidth. Use **wireless client mac-address** <*wgb-wireless-client-mac-address*> **deauthenticate** command on the wireless controller to deauthenticate the WGB wireless client.

Configuring Strong Password in Day0

It is required to set a strong password for WGB/uWGB after first login. The username and strong password should follow these rules:

1. Username length is between 1 and 32 characters.

2. Password length is between 8 to 120 characters.
3. Password must contain at least one uppercase character, one lowercase character, one digit, and one punctuation.
4. Password can contain alphanumeric characters and special characters (ASCII decimal code from 33 to 126), but the following special characters are not permitted: " (double quote), ' (single quote), ? (question mark).
5. Password cannot contain three sequential characters.
6. Password cannot contain three same characters consecutively.
7. Password cannot be the same as or reverse of the username.
8. New password must have at least four different characters compared to the current password.

For example, by default, the credential is

- username: Cisco
- password: Cisco
- enable password: Cisco

To reset the credential with the following strong password:

- username: demouser
- password: DemoP@ssw0rd
- enable password: DemoE^aP@ssw0rd

```
User Access Verification
Username: Cisco
Password: Cisco

% First Login: Please Reset Credentials

Current Password:Cisco
Current Enable Password:Cisco
New User Name:demouser
New Password:DemoP@ssw0rd
Confirm New Password:DemoP@ssw0rd
New Enable Password:DemoE^aP@ssw0rd
Confirm New Enable Password:DemoE^aP@ssw0rd

% Credentials changed, please re-login

[*04/18/2023 23:53:44.8926] chpasswd: password for user changed
[*04/18/2023 23:53:44.9074]
[*04/18/2023 23:53:44.9074] Management user configuration saved successfully
[*04/18/2023 23:53:44.9074]


User Access Verification
Username: demouser
Password: DemoP@ssw0rd
APFC58.9A15.C808>enable
Password:DemoE^aP@ssw0rd
APFC58.9A15.C808#
```

Note In above example, all passwords are displayed in plain text for demonstration purpose. In real case, they are hidden by asterisks (*).

Controller Configuration for WGB

For a WGB to join a wireless network, you need to configure specific settings on the WLAN and related policy profile on the controller.

Follow these steps to configure the Cisco Client Extensions option and set the support of Aironet IE in the WLAN:

1. Enter WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.

   ```
   #wlan profile-name
   ```

2. Configure the Cisco Client Extensions option and set the support of Aironet IE on the WLAN.

   ```
   #ccx aironet-iesupport
   ```

Note Without this configuration, WGB is not able to associate to AP.

Follow these steps to configure WLAN policy profile:

1. Enter wireless policy configuration mode.

   ```
   #wireless profile policy profile-policy
   ```

2. Assign the profile policy to the VLAN.

   ```
   #vlan vlan-id
   ```

3. Configure WGB VLAN client support.

   ```
   #wgb vlan
   ```

uWGB Image Upgrade

uWGB mode does not support TFTP or SFTP. To perform a software upgrade, follow these steps:

Procedure

Step 1 Connect a TFTP or SFTP server to wired 0 port of uWGB.

Step 2 Turn radio interfaces into Administratively Down state.

configure Dot11Radio <0|1> disable

Example:

```
#configure Dot11Radio 0 disable
#configure Dot11Radio 1 disable
```

Step 3 Convert uWGB to WGB mode.

configure Dot11Radio *slot_id* **mode wgb ssid-profile** *ssid_profile_name*

Example:

```
#configure Dot11Radio 1 mode wgb ssid-profile a_uwgb_demo_ssid

This command will reboot with downloaded configs.
Are you sure you want continue? <confirm>
```

Note
ssid_profile_name can be any existing SSID profile configured by users.

Step 4 After rebooting, assign a static IP address to the WGB.

configure ap address ipv4 static *IPv4_address netmask Gateway_IPv4_address*

Example:

```
#configure ap address ipv4 static 192.168.1.101 255.255.255.0 192.168.1.1
```

Step 5 Verify the ICMP ping works.

ping *server_IP*

Example:

```
#ping 192.168.1.20
Sending 5, 100-byte ICMP Echos to 192.168.1.20, timeout is 2 seconds

PING 192.168.1.20
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0.858/0.932/1.001 ms
```

Step 6 Upgrade the software.

archive download /reload <**tftp | sftp | http**>://*server_ip*/*file_path*

Step 7 Convert WGB back to uWGB.

configure Dot11Radio *slot_id* **mode uwgb** *wired_client_mac_addr* **ssid-profile** *ssid_profile_name*

Example:

```
#configure Dot11Radio 1 mode uwgb 00b4.9e00.a891 ssid-profile a_uwgb_demo_ssid
```

WGB Configuration

The typical WGB configuration involves the following steps:

1. Create an SSID profile.
2. Configure radio as workgroup, and associate the SSID profile to the radio.
3. Turn on the radio.

WGB uplink supports various security methods, including:

- Open (unsecured)
- PSK
- Dot1x (LEAP, PEAP, FAST-EAP, TLS)

Note Ensure that the below configuration order is followed when EAP-TLS security is desired on the WGB:

1. Configure the device username/password, NTP server, hostname, and valid IP address.
2. Create trustpoints and import the certificates using your preferred method.
3. (Optional) Configure the dot1x credentials.
4. Create the EAP profile and map the method, trustpoint name and dot1x credentials (optional).
5. Bind the EAP profile to the SSID profile.
6. Bind the SSID profile to the preferred radio.

Note If you make any modifications to the dot1x credential profile, trustpoint profile, or EAP profile, the changes do not take effect immediately. You must manually re-attach the EAP profile to the SSID profile for the changes to apply.

Use **configure ssid-profile <ssid_prof_name> ssid authentication eap profile <eap_prof_name> key-management <key_type>** command to re-attach the EAP profile to the SSID profile.

```
Device#configure ssid-profile <ssid_prof_name> ssid <ssid name> authentication eap profile
 <eap_prof_name> key-management <key_type>
```

The following is an example of Dot1x FAST-EAP configuration:

```
configure dot1x credential demo-cred username demouser1 password Dem0Pass!@
configure eap-profile demo-eap-profile dot1x-credential demo-cred
configure eap-profile demo-eap-profile method fast
configure ssid-profile demo-FAST ssid demo-fast authentication eap profile demo-eap-profile
 key-management wpa2
configure dot11radio 0 mode wgb ssid-profile demo-FAST
configure dot11radio 0 enable
```

The following sections provide detailed information about WGB configuration.

Configure IP address

Configure IPv4 address

- Use the **configure ap address** *ipv4 dhcp* command to configure IPv4 address using DHCP.

  ```
  Device#configure ap address ipv4 dhcp
  ```

- Use the **configure ap address** *ipv4 static ipv4_addr netmask gateway* command to configure the static IPv4 address. By doing so, you can manage the device using a wired interface without an uplink connection.

```
Device#configure ap address ipv4 static ipv4_addr netmask gateway
```

Verify current IP configuration

Use **show ip interface brief** command to view the current IP address configuration.

```
Device#show ip interface brief
```

Configure IPv6 address

Use the **configure ap address ipv6 static** *ipv6_addr prefixlen [gateway]* command to configure the static IPv6 address. This configuration allows you to manage the AP through a wired interface without uplink connection.

```
Device#configure ap address ipv6 static ipv6_addr prefixlen [gateway]
```

Enable IPv6 auto configuration

Use the **configure ap address ipv6 auto-config enable** command to enable the IPv6 auto configuration on the AP.

```
Device#configure ap address ipv6 auto-config enable
```

Note

- Use the **configure ap address ipv6 auto-config disable** command to disable the IPv6 auto configuration on the AP.
- Use the **configure ap address ipv6 auto-config enable** command to enable IPv6 SLAAC. Note that SLAAC does not apply to CoS of WGB. This command configures IPv6 address with DHCPv6 instead of SLAAC.

Configure IPv6 address using DHCP

Use the **configure ap address** *ipv6 dhcp* command to configure IPv6 address using DHCP.

```
Device#configure ap address ipv6 dhcp
```

Verify current IP configuration

Use the **show ipv6 interface brief** command to verify current IP address configuration.

```
Device#show ipv6 interface brief
```

Configure a Dot1X credential

Use the **configure dot1x credential** *profile-name* **username** *name* **password** *pwd* command to configure Dot1x credential.

```
Device#configure dot1x credential profile-name username name password pwd
```

Verify WGB EAP Dot1x profile

Use the **show wgb eap dot1x credential profile** command to view the status of WGB EAP Dot1x profile.

```
Device#show wgb eap dot1x credential profile
```

Deauthenticate WGB wired client

Use the **clear wgb client** {**all** | **single** *mac-addr*} command to deauthenticate WGB wired client.

```
Device#clear wgb client all
```

Configure an EAP profile

Perform these steps to configure an EAP profile:

1. Attach the Dot1x credential profile to the EAP profile.
2. Attach the EAP profile to the SSID profile.
3. Attach the SSID profile to the radio.

Procedure

Step 1 Use the **configure eap-profile** *profile-name* **method** {**fast** | **leap** | **peap** | **tls**} command to configure the EAP profile.

```
Device#configure eap-profile profile-name method { fast | leap | peap | tls}
```

Note
Choose an EAP profile method.

- fast
- peap, or
- tls.

Step 2 Use the **configure eap-profile** *profile-name* **trustpoint** {**default** | **name** *trustpoint-name*} command to attach the CA trustpoint for TLS. By default, the WGB uses the internal MIC certificate for authentication.

```
Device#configure eap-profile profile-name trustpoint { default | name trustpoint-name}
```

Step 3 Use the **configure eap-profile** *profile-name* **dot1x-credential** *profile-name* command to attach the dot1x-credential profile.

```
Device#configure eap-profile profile-name dot1x-credential profile-name
```

Step 4 [Optional] Use the **configure eap-profile** *profile-name* **delete** command to delete an EAP profile.

```
Device#configure eap-profile profile-name delete
```

Configure trustpoint manual enrollment for terminal

Procedure

Step 1 Use the **configure crypto pki trustpoint** *ca-server-name* **enrollment terminal** command to create a trustpoint in WGB.

```
Device#configure crypto pki trustpoint ca-server-name enrollment terminal
```

Step 2 Use the **configure crypto pki trustpoint** *ca-server-name* **authenticate** command to authenticate a trustpoint manually.

```
Device#configure crypto pki trustpoint ca-server-name authenticate
```

Enter the base 64 encoded CA certificate.

Enter **quit** to finish the certificate.

Note
If you use an intermediate certificate, import all the certificate chains in the trustpoint.

Example:

```
Device#configure crypto pki trustpoint demotp authenticate

Enter the base 64 encoded CA certificate.
....And end with the word "quit" on a line by itself....

-----BEGIN CERTIFICATE-----
[base64 encoded root CA certificate]
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
[base64 encoded intermediate CA certificate]
-----END CERTIFICATE-----
quit
```

Step 3 Use the **configure crypto pki trustpoint** *ca-server-name* **key-size** *key-length* command to configure a private key size.

```
Device#configure crypto pki trustpoint ca-server-name key-size key-length
```

Step 4 Use the **configure crypto pki trustpoint** *ca-server-name* **subject-name** *name* `[Optional]` *2ltr-country-code state-name locality org-name org-unit email* command to configure the subject-name.

```
Device#configure crypto pki trustpoint ca-server-name subject-name name [Optional] 2ltr-country-code
 state-name locality org-name org-unit email
```

Step 5 Use the **configure crypto pki trustpoint** *ca-server-name* **enroll** command to generate a private key and certificate signing request (CSR).

```
Device#configure crypto pki trustpoint ca-server-name enroll
```

Create the digitally signed certificate using the CSR output in the CA server.

Step 6 Use the **configure crypto pki trustpoint** *ca-server-name* **import certificate** command to import the signed certificate in WGB.

```
Device#configure crypto pki trustpoint ca-server-name import certificate
```

Enter the base 64 encoded CA certificate.

Enter **quit** to finish the certificate.

```
Device#quit
```

Step 7 [Optional] Use the **configure crypto pki trustpoint** *trustpoint-name* **delete** command to delete a trustpoint.

```
Device#configure crypto pki trustpoint trustpoint-name delete
```

Step 8 Use the **show crypto pki trustpoint** command to view the trustpoint summary.

```
Device#show crypto pki trustpoint
```

Step 9 Use the **show crypto pki trustpoint** *trustpoint-name* **certificate** command to view the content of the certificates that are created for a trustpoint.

```
Device#show crypto pki trustpoint trustpoint-name certificate
```

Configure trustpoint auto-enrollment for WGB

Procedure

Step 1 Use the **configure crypto pki trustpoint** *ca-server-name* **enrollment url** *ca-server-url* command to enroll a trustpoint in the WGB using the server URL.

```
Device#configure crypto pki trustpoint ca-server-name enrollment url ca-server-url
```

Step 2 Use the **configure crypto pki trustpoint** *ca-server-name* **authenticate** command to authenticate a trustpoint.

```
Device#configure crypto pki trustpoint ca-server-name authenticate
```

This command fetches the CA certificate from CA server automatically.

Step 3 Use the **configure crypto pki trustpoint** *ca-server-name* **key-size** *key-length* command to configure a private key size.

```
Device#configure crypto pki trustpoint ca-server-name key-size key-length
```

Step 4 Use the **configure crypto pki trustpoint** *ca-server-name* **subject-name** *name* `[Optional]` *2ltr-country-code state-name locality org-name org-unit email* command to configure the subject-name.

```
Device#configure crypto pki trustpoint ca-server-name subject-name name [Optional] 2ltr-country-code
 state-name locality org-name org-unit email
```

Step 5 Use the **configure crypto pki trustpoint** *ca-server-name* **enroll** command to enroll the trustpoint.

```
Device#configure crypto pki trustpoint ca-server-name enroll
```

Request the digitally signed certificate from the CA server.

Step 6 Use the **configure crypto pki trustpoint** *ca-server-name* **auto-enroll enable** *renew-percentage* command to enable auto-enroll.

```
Device#configure crypto pki trustpoint ca-server-name auto-enroll enable renew-percentage
```

Note
Use the **configure crypto pki trustpoint** *ca-server-name* **auto-enroll disable** command to disable the auto-enroll.

Step 7 [Optional] Use the **configure crypto pki trustpoint** *trustpoint-name* **delete** command to delete a trustpoint.

```
Device#configure crypto pki trustpoint trustpoint-name delete
```

Step 8 Use the **show crypto pki trustpoint** command to view the trustpoint summary.

```
Device#show crypto pki trustpoint
```

Step 9 Use the **show crypto pki trustpoint** *trustpoint-name* **certificate** command to view the details of the certificate for a specific trustpoint.

```
Device#show crypto pki trustpoint trustpoint-name certificate
```

Step 10 Use the **show crypto pki timers** command to view the public key infrastructure (PKI) timer information.

show crypto pki timers

```
Device#show crypto pki timers
```

Configure manual certificate enrollment using TFTP server

Procedure

Step 1 Specify the enrollment method.

Use the **configure crypto pki trustpoint** *ca-server-name* **enrollment tftp** *tftp-addr/file-name* command to retrieve the CA and client certificate for a trustpoint.

```
Device#configure crypto pki trustpoint ca-server-name enrollment tftp tftp-addr/file-name
```

Step 2 Use the **configure crypto pki trustpoint** *ca-server-name* **authenticate** command to authenticate a trustpoint manually.

```
Device#configure crypto pki trustpoint ca-server-name authenticate
```

This retrieves and authenticates the CA certificate from the specified TFTP server. If the file specification is included, the WGB adds the extension **.ca** to the specified filename.

Step 3 Use the **configure crypto pki trustpoint** *ca-server-name* **key-size** *key-length* command to configure a private key size.

```
Device#configure crypto pki trustpoint ca-server-name key-size key-length
```

Step 4 Use the **configure crypto pki trustpoint** *ca-server-name* **subject-name** *name* `[Optional]` *2ltr-country-code state-name locality org-name org-unit email* command to configure the subject-name.

```
Device#configure crypto pki trustpoint ca-server-name subject-name name [Optional] 2ltr-country-code
 state-name locality org-name org-unit email
```

Step 5 Use the **configure crypto pki trustpoint** *ca-server-name* **enroll** command to generate a private key and Certificate Signing Request (CSR).

```
Device#configure crypto pki trustpoint ca-server-name enroll
```

This generates certificate request and sends the request to the TFTP server. The filename to be written is appended with the **.req** extension.

Step 6 Use the **configure crypto pki trustpoint** *ca-server-name* **import certificate** command to import the signed certificate in WGB.

```
Device#configure crypto pki trustpoint ca-server-name import certificate
```

The console terminal uses TFTP to import a certificate and the WGB tries to get the approved certificate from the TFTP. The filename to be written is appended with the **.crt** extension.

Step 7 Use the **show crypto pki trustpoint** command to view the trustpoint summary.

```
Device#show crypto pki trustpoint
```

Step 8 Use the **show crypto pki trustpoint** *trustpoint-name* **certificate** command to view the content of the certificates that are created for a trustpoint.

```
Device#show crypto pki trustpoint trustpoint-name certificate
```

SSID configuration

SSID configuration consists of the following two parts:

1. Create an SSID profile, on page 35
2. Configuring Radio Interface for Workgroup Bridges, on page 36

Create an SSID profile

Choose one of these authentication protocols to configure the SSID profile:

1. Open authentication
2. PSK authentication
   - PSK WPA2 authentication
   - PSK Dot11r authentication, and
   - PSK Dot11w authentication.
3. Dot1x authentication

Configure an SSID profile using open authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *radio-serv-name* **authentication** *open* command to configure an SSID profile using open authentication.

```
Device#configure ssid-profile ssid-profile-name ssid radio-serv-name authentication open
```

Configure an SSID profile using PSK authentication

Choose one of these authentication protocols to configure an SSID profile using PSK authentication:

- configure an SSID profile using PSK WPA2 authentication
- configure an SSID profile using PSK Dot11r authentication, and
- configure an SSID profile using PSK Dot11w authentication .

Configure an SSID profile using PSK WPA2 authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management wpa2** command to configure an SSID profile using PSK WPA2 authentication.

```
Device#configure ssid-profile ssid-profile-name ssid SSID_name authentication psk
preshared-key key-management wpa2
```

Configure an SSID profile using PSK Dot11r authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management dot11r** command to configure an SSID profile using PSK Dot11r authentication.

```
Device#configure ssid-profile ssid-profile-name ssid SSID_name authentication psk
preshared-key key-management dot11r
```

Configure an SSID profile using PSK Dot11w authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management dot11w** command to configure an SSID profile using PSK Dot11w authentication

```
Device#configure ssid-profile ssid-profile-name ssid SSID_name authentication psk
preshared-key key-management dot11w
```

Configure an SSID profile using Dot1x authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *radio-serv-name* **authentication eap profile** *eap-profile-name* **key-management** {**dot11r** | **wpa2** | **dot11w** {**optional | required**}} command to configure an SSID profile using Dot1x authentication.

```
Device#configure ssid-profile ssid-profile-name ssid radio-serv-name authentication eap
profile eap-profile-name key-management { dot11r | wpa2 | dot11w { optional | required}}
```

Configure an SSID profile using Dot1x EAP-PEAP authentication

Here is an example that shows the configuration of an SSID profile using Dot1x EAP-PEAP authentication:

```
Device#configure dot1x credential c1 username wgbusr password cisco123456
Device#configure eap-profile p1 dot1x-credential c1
Device#configure eap-profile p1 method peap
Device#configure ssid-profile iot-peap ssid iot-peap authentication eap profile p1
key-management wpa2
```

Configuring Radio Interface for Workgroup Bridges

- From the available two radio interfaces, before configuring WGB mode on one radio interface, configure the other radio interface to root-ap mode.

  Map a radio interface as root-ap by entering this command:

  # **configure dot11radio** *radio-slot-id* **mode root-ap**

  Example

  ```
  # configure dot11radio 0 mode root-ap
  ```

Note When an active SSID or EAP profile is modified, you need to reassociate the profile to the radio interface for the updated profile to be active.

- Map a radio interface to a WGB SSID profile by entering this command:

  # **configure dot11radio** *radio-slot-id* **mode wgb ssid-profile** *ssid-profile-name*

  Example

  ```
  # configure dot11radio 1 mode wgb ssid-profile psk_ssid
  ```

- Configure a radio interface by entering this command:

  # **configure dot11radio** *radio-slot-id*{ **enable** | **disable** }

  Example

  ```
  # configure dot11radio 0 disable
  ```

Note Only one radio or slot is allowed to operate in WGB mode.

Configuring WGB/uWGB Timer

The timer configuration CLIs are common for both WGB and uWGB. Use the following commands to configure timers:

- Configure the WGB association response timeout by entering this command:

  # **configure wgb association response timeout** *response-millisecs*

  The default value is 100 milliseconds. The valid range is between 100 and 5000 milliseconds.

- Configure the WGB authentication response timeout by entering this command:

  # **configure wgb authentication response timeout** *response-millisecs*

  The default value is 100 milliseconds. The valid range is between 100 and 5000 milliseconds.

- Configure the WGB EAP timeout by entering this command:

  # **configure wgb eap timeout** *timeout-secs*

  The default value is 3 seconds. The valid range is between 2 and 60 seconds.

- Configure the WGB bridge client response timeout by entering this command:

  # **configure wgb bridge client timeout** *timeout-secs*

  Default timeout value is 300 seconds. The valid range is between 10 and 1000000 seconds.

uWGB Configuration

The universal WGB is able to interoperate with non-Cisco access points using uplink radio MAC address, thus the universal workgroup bridge role supports only one wired client.

Most WGB configurations apply to uWGB. The only difference is that you configure wired client's MAC address with the following command:

configure dot11 <**0**|**1**> **mode uwgb** <*uwgb_wired_client_mac_address*> **ssid-profile** <*ssid-profile*>

The following is an example of Dot1x FAST-EAP configuration:

```
configure dot1x credential demo-cred username demouser1 password Dem0Pass!@
configure eap-profile demo-eap-profile dot1x-credential demo-cred
configure eap-profile demo-eap-profile method fast
configure ssid-profile demo-FAST ssid demo-fast authentication eap profile demo-eap-profile
 key-management wpa2
configure dot11radio 0 mode uwgb fc58.220a.0704 ssid-profile demo-FAST
configure dot11radio 0 enable
```

The following sections provide detailed information about uWGB configuration.

Configure IP address

Configure IPv4 address

- Use the **configure ap address** *ipv4 dhcp* command to configure IPv4 address using DHCP.

  ```
  Device#configure ap address ipv4 dhcp
  ```

- Use the **configure ap address** *ipv4 static ipv4_addr netmask gateway* command to configure the static IPv4 address. By doing so, you can manage the device using a wired interface without an uplink connection.

  ```
  Device#configure ap address ipv4 static ipv4_addr netmask gateway
  ```

Verify current IP configuration

Use **show ip interface brief** command to view the current IP address configuration.

```
Device#show ip interface brief
```

Configure IPv6 address

Use the **configure ap address ipv6 static** *ipv6_addr prefixlen [gateway]* command to configure the static IPv6 address. This configuration allows you to manage the AP through a wired interface without uplink connection.

```
Device#configure ap address ipv6 static ipv6_addr prefixlen [gateway]
```

Enable IPv6 auto configuration

Use the **configure ap address ipv6 auto-config enable** command to enable the IPv6 auto configuration on the AP.

```
Device#configure ap address ipv6 auto-config enable
```

Note

- Use the **configure ap address ipv6 auto-config disable** command to disable the IPv6 auto configuration on the AP.
- Use the **configure ap address ipv6 auto-config enable** command to enable IPv6 SLAAC. Note that SLAAC does not apply to CoS of WGB. This command configures IPv6 address with DHCPv6 instead of SLAAC.

Configure IPv6 address using DHCP

Use the **configure ap address** *ipv6 dhcp* command to configure IPv6 address using DHCP.

```
Device#configure ap address ipv6 dhcp
```

Verify current IP configuration

Use the **show ipv6 interface brief** command to verify current IP address configuration.

```
Device#show ipv6 interface brief
```

Configure a Dot1X credential

Use the **configure dot1x credential** *profile-name* **username** *name* **password** *pwd* command to configure Dot1x credential.

```
Device#configure dot1x credential profile-name username name password pwd
```

Verify WGB EAP Dot1x profile

Use the **show wgb eap dot1x credential profile** command to view the status of WGB EAP Dot1x profile.

```
Device#show wgb eap dot1x credential profile
```

Configure an EAP profile

Perform these steps to configure an EAP profile:

1. Attach the Dot1x credential profile to the EAP profile.
2. Attach the EAP profile to the SSID profile.
3. Attach the SSID profile to the radio.

Procedure

Step 1 Use the **configure eap-profile** *profile-name* **method** {**fast** | **leap** | **peap** | **tls**} command to configure the EAP profile.

```
Device#configure eap-profile profile-name method { fast | leap | peap | tls}
```

Note
Choose an EAP profile method.

- fast
- peap, or
- tls.

Step 2 Use the **configure eap-profile** *profile-name* **trustpoint** {**default** | **name** *trustpoint-name*} command to attach the CA trustpoint for TLS. By default, the WGB uses the internal MIC certificate for authentication.

```
Device#configure eap-profile profile-name trustpoint { default | name trustpoint-name}
```

Step 3 Use the **configure eap-profile** *profile-name* **dot1x-credential** *profile-name* command to attach the dot1x-credential profile.

```
Device#configure eap-profile profile-name dot1x-credential profile-name
```

Step 4 [Optional] Use the **configure eap-profile** *profile-name* **delete** command to delete an EAP profile.

```
Device#configure eap-profile profile-name delete
```

Configure trustpoint manual enrollment for terminal

Procedure

Step 1 Use the **configure crypto pki trustpoint** *ca-server-name* **enrollment terminal** command to create a trustpoint in WGB.

```
Device#configure crypto pki trustpoint ca-server-name enrollment terminal
```

Step 2 Use the **configure crypto pki trustpoint** *ca-server-name* **authenticate** command to authenticate a trustpoint manually.

```
Device#configure crypto pki trustpoint ca-server-name authenticate
```

Enter the base 64 encoded CA certificate.

Enter **quit** to finish the certificate.

Note
If you use an intermediate certificate, import all the certificate chains in the trustpoint.

Example:

```
Device#configure crypto pki trustpoint demotp authenticate

Enter the base 64 encoded CA certificate.
....And end with the word "quit" on a line by itself....

-----BEGIN CERTIFICATE-----
[base64 encoded root CA certificate]
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
[base64 encoded intermediate CA certificate]
-----END CERTIFICATE-----
quit
```

Step 3 Use the **configure crypto pki trustpoint** *ca-server-name* **key-size** *key-length* command to configure a private key size.

```
Device#configure crypto pki trustpoint ca-server-name key-size key-length
```

Step 4 Use the **configure crypto pki trustpoint** *ca-server-name* **subject-name** *name* `[Optional]` *2ltr-country-code state-name locality org-name org-unit email* command to configure the subject-name.

```
Device#configure crypto pki trustpoint ca-server-name subject-name name [Optional] 2ltr-country-code
 state-name locality org-name org-unit email
```

Step 5 Use the **configure crypto pki trustpoint** *ca-server-name* **enroll** command to generate a private key and certificate signing request (CSR).

```
Device#configure crypto pki trustpoint ca-server-name enroll
```

Create the digitally signed certificate using the CSR output in the CA server.

Step 6 Use the **configure crypto pki trustpoint** *ca-server-name* **import certificate** command to import the signed certificate in WGB.

```
Device#configure crypto pki trustpoint ca-server-name import certificate
```

Enter the base 64 encoded CA certificate.

Enter **quit** to finish the certificate.

```
Device#quit
```

Step 7 [Optional] Use the **configure crypto pki trustpoint** *trustpoint-name* **delete** command to delete a trustpoint.

```
Device#configure crypto pki trustpoint trustpoint-name delete
```

Step 8 Use the **show crypto pki trustpoint** command to view the trustpoint summary.

```
Device#show crypto pki trustpoint
```

Step 9 Use the **show crypto pki trustpoint** *trustpoint-name* **certificate** command to view the content of the certificates that are created for a trustpoint.

```
Device#show crypto pki trustpoint trustpoint-name certificate
```

Configure trustpoint auto-enrollment for WGB

Procedure

Step 1 Use the **configure crypto pki trustpoint** *ca-server-name* **enrollment url** *ca-server-url* command to enroll a trustpoint in the WGB using the server URL.

```
Device#configure crypto pki trustpoint ca-server-name enrollment url ca-server-url
```

Step 2 Use the **configure crypto pki trustpoint** *ca-server-name* **authenticate** command to authenticate a trustpoint.

```
Device#configure crypto pki trustpoint ca-server-name authenticate
```

This command fetches the CA certificate from CA server automatically.

Step 3 Use the **configure crypto pki trustpoint** *ca-server-name* **key-size** *key-length* command to configure a private key size.

```
Device#configure crypto pki trustpoint ca-server-name key-size key-length
```

Step 4 Use the **configure crypto pki trustpoint** *ca-server-name* **subject-name** *name* `[Optional]` *2ltr-country-code state-name locality org-name org-unit email* command to configure the subject-name.

```
Device#configure crypto pki trustpoint ca-server-name subject-name name [Optional] 2ltr-country-code
 state-name locality org-name org-unit email
```

Step 5 Use the **configure crypto pki trustpoint** *ca-server-name* **enroll** command to enroll the trustpoint.

```
Device#configure crypto pki trustpoint ca-server-name enroll
```

Request the digitally signed certificate from the CA server.

Step 6 Use the **configure crypto pki trustpoint** *ca-server-name* **auto-enroll enable** *renew-percentage* command to enable auto-enroll.

```
Device#configure crypto pki trustpoint ca-server-name auto-enroll enable renew-percentage
```

Note
Use the **configure crypto pki trustpoint** *ca-server-name* **auto-enroll disable** command to disable the auto-enroll.

Step 7 [Optional] Use the **configure crypto pki trustpoint** *trustpoint-name* **delete** command to delete a trustpoint.

```
Device#configure crypto pki trustpoint trustpoint-name delete
```

Step 8 Use the **show crypto pki trustpoint** command to view the trustpoint summary.

```
Device#show crypto pki trustpoint
```

Step 9 Use the **show crypto pki trustpoint** *trustpoint-name* **certificate** command to view the details of the certificate for a specific trustpoint.

```
Device#show crypto pki trustpoint trustpoint-name certificate
```

Step 10 Use the **show crypto pki timers** command to view the public key infrastructure (PKI) timer information.

show crypto pki timers

```
Device#show crypto pki timers
```

Configure manual certificate enrollment using TFTP server

Procedure

Step 1 Specify the enrollment method.

Use the **configure crypto pki trustpoint** *ca-server-name* **enrollment tftp** *tftp-addr/file-name* command to retrieve the CA and client certificate for a trustpoint.

```
Device#configure crypto pki trustpoint ca-server-name enrollment tftp tftp-addr/file-name
```

Step 2 Use the **configure crypto pki trustpoint** *ca-server-name* **authenticate** command to authenticate a trustpoint manually.

```
Device#configure crypto pki trustpoint ca-server-name authenticate
```

This retrieves and authenticates the CA certificate from the specified TFTP server. If the file specification is included, the WGB adds the extension **.ca** to the specified filename.

Step 3 Use the **configure crypto pki trustpoint** *ca-server-name* **key-size** *key-length* command to configure a private key size.

```
Device#configure crypto pki trustpoint ca-server-name key-size key-length
```

Step 4 Use the **configure crypto pki trustpoint** *ca-server-name* **subject-name** *name* `[Optional]` *2ltr-country-code state-name locality org-name org-unit email* command to configure the subject-name.

```
Device#configure crypto pki trustpoint ca-server-name subject-name name [Optional] 2ltr-country-code
 state-name locality org-name org-unit email
```

Step 5 Use the **configure crypto pki trustpoint** *ca-server-name* **enroll** command to generate a private key and Certificate Signing Request (CSR).

```
Device#configure crypto pki trustpoint ca-server-name enroll
```

This generates certificate request and sends the request to the TFTP server. The filename to be written is appended with the **.req** extension.

Step 6 Use the **configure crypto pki trustpoint** *ca-server-name* **import certificate** command to import the signed certificate in WGB.

```
Device#configure crypto pki trustpoint ca-server-name import certificate
```

The console terminal uses TFTP to import a certificate and the WGB tries to get the approved certificate from the TFTP. The filename to be written is appended with the **.crt** extension.

Step 7 Use the **show crypto pki trustpoint** command to view the trustpoint summary.

```
Device#show crypto pki trustpoint
```

Step 8 Use the **show crypto pki trustpoint** *trustpoint-name* **certificate** command to view the content of the certificates that are created for a trustpoint.

```
Device#show crypto pki trustpoint trustpoint-name certificate
```

SSID configuration

SSID configuration consists of the following two parts:

1. Create an SSID profile, on page 35
2. Configuring Radio Interface for uWGB, on page 44

Create an SSID profile

Choose one of these authentication protocols to configure the SSID profile:

1. Open authentication
2. PSK authentication
   - PSK WPA2 authentication
   - PSK Dot11r authentication, and
   - PSK Dot11w authentication.
3. Dot1x authentication

Configure an SSID profile using open authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *radio-serv-name* **authentication** *open* command to configure an SSID profile using open authentication.

```
Device#configure ssid-profile ssid-profile-name ssid radio-serv-name authentication open
```

Configure an SSID profile using PSK authentication

Choose one of these authentication protocols to configure an SSID profile using PSK authentication:

- configure an SSID profile using PSK WPA2 authentication
- configure an SSID profile using PSK Dot11r authentication, and
- configure an SSID profile using PSK Dot11w authentication .

Configure an SSID profile using PSK WPA2 authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management wpa2** command to configure an SSID profile using PSK WPA2 authentication.

```
Device#configure ssid-profile ssid-profile-name ssid SSID_name authentication psk
preshared-key key-management wpa2
```

Configure an SSID profile using PSK Dot11r authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management dot11r** command to configure an SSID profile using PSK Dot11r authentication.

```
Device#configure ssid-profile ssid-profile-name ssid SSID_name authentication psk
preshared-key key-management dot11r
```

Configure an SSID profile using PSK Dot11w authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *SSID_name* **authentication psk** *preshared-key* **key-management dot11w** command to configure an SSID profile using PSK Dot11w authentication

```
Device#configure ssid-profile ssid-profile-name ssid SSID_name authentication psk
preshared-key key-management dot11w
```

Configure an SSID profile using Dot1x authentication

Use the **configure ssid-profile** *ssid-profile-name* **ssid** *radio-serv-name* **authentication eap profile** *eap-profile-name* **key-management** {**dot11r** | **wpa2** | **dot11w** {**optional | required**} } command to configure an SSID profile using Dot1x authentication.

```
Device#configure ssid-profile ssid-profile-name ssid radio-serv-name authentication eap
profile eap-profile-name key-management { dot11r | wpa2 | dot11w { optional | required}}
```

Configure an SSID profile using Dot1x EAP-PEAP authentication

Here is an example that shows the configuration of an SSID profile using Dot1x EAP-PEAP authentication:

```
Device#configure dot1x credential c1 username wgbusr password cisco123456
Device#configure eap-profile p1 dot1x-credential c1
Device#configure eap-profile p1 method peap
Device#configure ssid-profile iot-peap ssid iot-peap authentication eap profile p1
key-management wpa2
```

Configuring Radio Interface for uWGB

- From the available two radio interfaces, before configuring WGB mode on one radio interface, configure the other radio interface to root-ap mode.

  Map a radio interface as root-ap by entering this command:

configure dot11radio *radio-slot-id* **mode root-ap**

Example

```
# configure dot11radio 0 mode root-ap
```

Note When an active SSID or EAP profile is modified, you need to reassociate the profile to the radio interface for the updated profile to be active.

- Map a radio interface to a WGB SSID profile by entering this command:

  # **configure dot11radio** *radio-slot-id* **mode uwgb** *uwgb-wired-client-mac-address* **ssid-profile** *ssid-profile-name*

- Configure a radio interface by entering this command:

  # **configure dot11radio** *radio-slot-id*{ **enable** | **disable** }

  Example

```
# configure dot11radio 0 disable
```

Note After configuring the uplink to the SSID profile, we recommend you to disable and enable the radio for the changes to be active.

Note Only one radio or slot is allowed to operate in uWGB or WGB mode.

Converting Between WGB and uWGB

To convert from WGB to uWGB, use the following command:

#**configure dot11radio** <**0**|**1**> **mode uwgb** <*WIRED_CLIENT_MAC*> **ssid-profile** <*SSID_PROFILE_NAME*>

To convert from uWGB to WGB, use the following command. This conversion involves a reboot of the AP.

#**configure Dot11Radio 1 mode wgb ssid-profile** <*SSID_PROFILE_NAME*>

```
This command will reboot with downloaded configs.
Are you sure you want continue? [confirm]
```

LED Pattern

Two new LED patterns are added to IW9167EH WGB mode:

- When WGB is in disassociated state, the System LED is blinking RED.
- When WGB makes association to parent AP, System LED turns to solid GREEN.

Configuring HT Speed Limit

In WGB field moving case deployment, you can manually set a transmission rate limit with High Throughput (HT) Modulation and Coding Scheme (MCS).

The following is an example to configure WGB to transmit with 802.11n HT m4. m5. rate:

Config dot11radio [**1**|**2**] **802.11ax disable**

Config dot11radio [**1**|**2**] **802.11ac disable**

Config dot11radio [**1**|**2**] **speed ht-mcs m4. m5.**

WGB also supports to configure legacy rates.

- For 802.11b/g, the legacy rates are configured as following:

```
configure dot11radio 0 speed legacy-rate
1.0 Allow 1.0 Mb/s rate
11.0 Allow 11.0 Mb/s rate
12.0 Allow 12.0 Mb/s rate
18.0 Allow 18.0 Mb/s rate
2.0 Allow 2.0 Mb/s rate
24.0 Allow 24.0 Mb/s rate
36.0 Allow 36.0 Mb/s rate
48.0 Allow 48.0 Mb/s rate
5.5 Allow 5.5 Mb/s rate
54.0 Allow 54.0 Mb/s rate
6.0 Allow 6.0 Mb/s rate
9.0 Allow 9.0 Mb/s rate
basic-1.0 Require 1.0 Mb/s rate
basic-11.0 Require 11.0 Mb/s rate
basic-12.0 Require 12.0 Mb/s rate
basic-18.0 Require 18.0 Mb/s rate
basic-2.0 Require 2.0 Mb/s rate
basic-24.0 Require 24.0 Mb/s rate
basic-36.0 Require 36.0 Mb/s rate
basic-48.0 Require 48.0 Mb/s rate
basic-5.5 Require 5.5 Mb/s rate
basic-54.0 Require 54.0 Mb/s rate
basic-6.0 Require 6.0 Mb/s rate
basic-9.0 Require 9.0 Mb/s rate
default Set default legacy rates
```

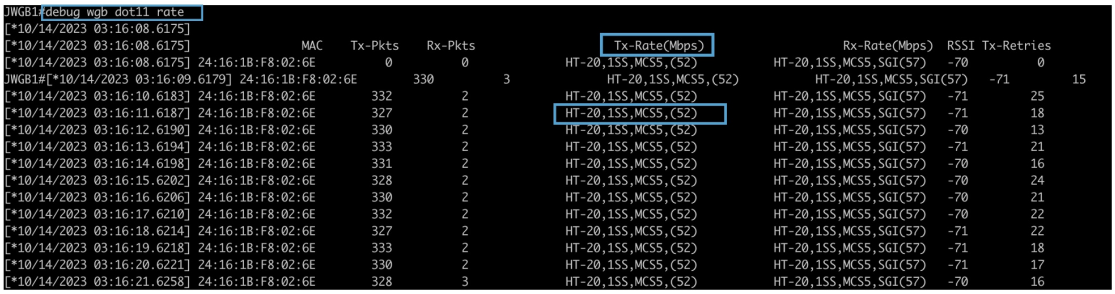
- For 802.11a, the legacy rates are configured as following:

```
configure dot11radio [1|2] speed legacy-rate
12.0 Allow 12.0 Mb/s rate
18.0 Allow 18.0 Mb/s rate
24.0 Allow 24.0 Mb/s rate
36.0 Allow 36.0 Mb/s rate
48.0 Allow 48.0 Mb/s rate
54.0 Allow 54.0 Mb/s rate
6.0 Allow 6.0 Mb/s rate
9.0 Allow 9.0 Mb/s rate
basic-12.0 Require 12.0 Mb/s rate
basic-18.0 Require 18.0 Mb/s rate
basic-24.0 Require 24.0 Mb/s rate
basic-36.0 Require 36.0 Mb/s rate
basic-48.0 Require 48.0 Mb/s rate
basic-54.0 Require 54.0 Mb/s rate
basic-6.0 Require 6.0 Mb/s rate
```

```
basic-9.0 Require 9.0 Mb/s rate
default Set default legacy rates
```

Legacy rate is used by 802.11 management frame and control frame. WGB legacy rates should match AP's legacy rates, or at least, having overlap between these two rate sets. Otherwise, WGB association will be rejected due to mismatched rates.

To check WGB Tx MCS rate, use the **debug wgb dot11 rate** command. The following example shows the output of this command.



Radio Statistics Commands

The **debug wgb dot11 rate**command displays debugging information related to data rates negotiated. It helps troubleshoot connectivity, performance, or roaming issues by showing how the WGB selects and uses data rates when communicating with the access point.

```
Device# debug wgb dot11 rate

[*03/13/2023 18:00:08.7814]                MAC    Tx-Pkts    Rx-Pkts
Tx-Rate(Mbps)                    Rx-Rate(Mbps)  RSSI   SNR Tx-Retries
[*03/13/2023 18:00:08.7814] FC:58:9A:17:C2:51        0         0      HE-20,2SS,MCS6,GI0.8
 (154)       HE-20,3SS,MCS4,GI0.8 (154)   -30    62          0
[*03/13/2023 18:00:09.7818] FC:58:9A:17:C2:51        0         0      HE-20,2SS,MCS6,GI0.8
 (154)       HE-20,3SS,MCS4,GI0.8 (154)   -30    62          0
```

In this example, FC:58:9A:17:C2:51 is the parent AP radio MAC.

The **show interfaces dot11Radio** *slot-id***statistics** command displays detailed statistics for a wireless radio interface. It provides information such as transmitted and received packets, errors, retries, signal quality, and other performance metrics. This is useful for monitoring the health of the radio interface, identifying connectivity issues, and troubleshooting wireless performance.

```
Device# show interfaces dot11Radio 1 statistics

Dot11Radio Statistics:
        DOT11 Statistics (Cumulative Total/Last 5 Seconds):
RECEIVER                                TRANSMITTER
Host Rx K Bytes:         965570/0       Host Tx K Bytes:        1611903/0
Unicasts Rx:             379274/0       Unicasts Tx:            2688665/0
Broadcasts Rx:          3166311/0       Broadcasts Tx:                0/0
Beacons Rx:           722130099/1631    Beacons Tx:           367240960/784
Probes Rx:            588627347/2224    Probes Tx:             78934926/80
Multicasts Rx:          3231513/0       Multicasts Tx:            53355/0
Mgmt Packets Rx:      764747086/1769    Mgmt Packets Tx:      446292853/864
Ctrl Frames Rx:         7316214/5       Ctrl Frames Tx:               0/0
RTS received:                 0/0       RTS transmitted:              0/0
Duplicate frames:             0/0       CTS not received:             0/0
MIC errors:                   0/0       WEP errors:             2279546/0
```

```
FCS errors:                  0/0        Retries:                896973/0
Key Index errors:            0/0        Tx Failures:              8871/0
                                        Tx Drops:                    0/0

Rate Statistics for Radio::
[Legacy]:
6 Mbps:
 Rx Packets:     159053/0            Tx Packets:      88650/0
                                     Tx Retries:       2382/0
9 Mbps:
 Rx Packets:         43/0            Tx Packets:         23/0
                                     Tx Retries:         71/0
12 Mbps:
 Rx Packets:          1/0            Tx Packets:        119/0
                                     Tx Retries:        185/0
18 Mbps:
 Rx Packets:          0/0            Tx Packets:          5/0
                                     Tx Retries:        134/0
24 Mbps:
 Rx Packets:        235/0            Tx Packets:      20993/0
                                     Tx Retries:       5048/0
36 Mbps:
 Rx Packets:          0/0            Tx Packets:        781/0
                                     Tx Retries:        227/0
54 Mbps:
 Rx Packets:        133/0            Tx Packets:       9347/0
                                     Tx Retries:       1792/0

[SU]:
M0:
 Rx Packets:          7/0            Tx Packets:          0/0
                                     Tx Retries:          6/0
M1:
 Rx Packets:       1615/0            Tx Packets:      35035/0
                                     Tx Retries:       3751/0
M2:
 Rx Packets:      15277/0            Tx Packets:     133738/0
                                     Tx Retries:      22654/0
M3:
 Rx Packets:      10232/0            Tx Packets:       1580/0
                                     Tx Retries:      21271/0
M4:
 Rx Packets:     218143/0            Tx Packets:     190408/0
                                     Tx Retries:      36444/0
M5:
 Rx Packets:     399283/0            Tx Packets:     542491/0
                                     Tx Retries:     164048/0
M6:
 Rx Packets:    3136519/0            Tx Packets:     821537/0
                                     Tx Retries:     329003/0
M7:
 Rx Packets:    1171128/0            Tx Packets:     303414/0
                                     Tx Retries:     154014/0


Beacons missed: 0-30s 31-60s 61-90s 90s+
                     2      0      0    0
```

The **show wgb dot11 uplink latency** command displays latency statistics for the Workgroup Bridge (WGB) uplink connection to the access point (AP). It helps measure the time taken for frames to traverse from the WGB to the AP, providing insight into wireless link performance and potential delay issues.

```
AP# show wgb dot11 uplink latency

Latency Group Total Packets Total Latency Excellent(0-8) Very Good(8-16) Good (16-32 ms)
Medium (32-64ms) Poor (64-256 ms) Very Poor (256+ ms)
        AC_BK             0             0              0               0               0
              0               0                0
        AC_BE          1840       4243793           1809              10              14
              7               0                0
        AC_VI             0             0              0               0               0
              0               0                0
        AC_VO            24         54134             24               0               0
              0               0                0
```

The **show wgb dot11 uplink** command displays information about the Workgroup Bridge (WGB) uplink to the access point (AP). It provides details such as the associated SSID, BSSID, channel, signal strength, data rates, authentication type, and overall status of the uplink connection. This is useful for verifying connectivity and monitoring the WGB's wireless link to the AP.

```
AP# show wgb dot11 uplink

HE Rates: 1SS:M0-11 2SS:M0-11
Additional info for client 8C:84:42:92:FF:CF
RSSI: -24
PS  : Legacy (Awake)
Tx Rate: 278730 Kbps
Rx Rate: 410220 Kbps
VHT_TXMAP: 65530
CCX Ver: 5
Rx Key-Index Errs: 0
             mac     intf TxData TxUC TxBytes TxFail TxDcrd TxCumRetries MultiRetries
MaxRetriesFail RxData RxBytes RxErr                 TxRt(Mbps)                 RxRt(Mbps)
  LER PER stats_ago
8C:84:42:92:FF:CF wbridge1   1341 1341  184032      0      0          543            96
         0    317   33523     0 HE-40,2SS,MCS6,GI0.8 (309) HE-40,2SS,MCS9,GI0.8 (458) 27272
   0  1.370000
Per TID packet statistics for client 8C:84:42:92:FF:CF
Priority Rx Pkts Tx Pkts Rx(last 5 s) Tx (last 5 s)
       0      35    1314            0             8
       1       0       0            0             0
       2       0       0            0             0
       3       0       0            0             0
       4       0       0            0             0
       5       0       0            0             0
       6     182      24            1             0
       7       3       3            0             0
Rate Statistics:
Rate-Index    Rx-Pkts    Tx-Pkts Tx-Retries
         0         99          3          0
         4          1          1          9
         5         21         39         35
         6         31        185         64
         7         26        124         68
         8         28        293         82
         9         77        401        151
        10         32        140         97
        11          2        156         37
```

Syslog

Syslogs are a category of protocols that send event data logs to a centralized location for storage and analysis. These are widely used for monitoring and troubleshooting network devices by capturing event messages. The term Syslog may also refer to the protocol itself or the system that implements it.

- Protocol Type: Syslog is a standardized protocol commonly used for logging system events.
- Transport Protocol: Currently, Syslog supports only UDP mode for data transmission.
- Debug Log Collection: When the debug command is enabled on a WGB, it collects debug logs and sends them to the Syslog server.
- Log Categorization: Logs sent to the Syslog server from WGB are categorized under the "kernel facility" and logged at the "warning level."

Event Logging

For WGB field deployment, event logging will collect useful information (such as WGB state change and packets rx/tx) to analyze and provide log history to present context of problem, especially in roaming cases.

You can configure WGB trace filter for all management packet types, including probe, auth, assoc, eap, dhcp, icmp, and arp. To enable or disable WGB trace, use the following command:

#**config wgb event trace** {**enable**|**disable**}

Four kinds of event types are supported:

- **Basic event**: covers most WGB basic level info message
- **Detail event**: covers basic event and additional debug level message
- **Trace event**: recording wgb trace event if enabled
- **All event**: bundle trace event and detail event

The log format is [*timestamp*] *module*:*level* <*event log string*>.

When abnormal situations happen, the eventlog messages can be dumped manually to memory by using the following show command which also displays WGB logging:

#**show wgb event** [**basic**|**detail**|**trace**|**all**]

The following example shows the output of **show wgb event all**:

```
APC0F8.7FE5.F3C0#show wgb event all
[*08/16/2023 08:18:25.167578] UP_EVT:4 R1 IFC:58:9A:17:B3:E7] parent_rssi: -42 threshold:
-70
[*08/16/2023 08:18:25.329223] UP_EVT:4 R1 State CONNECTED to SCAN_START
[*08/16/2023 08:18:25.329539] UP_EVT:4 R1 State SCAN_START to STOPPED
[*08/16/2023 08:18:25.330002] UP_DRV:1 R1 WGB UPLINK mode stopped
[*08/16/2023 08:18:25.629405] UP_DRV:1 R1 Delete client FC:58:9A:17:B3:E7
[*08/16/2023 08:18:25.736718] UP_CFG:8 R1 configured for standard: 7
[*08/16/2023 08:18:25.989936] UP_CFG:4 R1 band 1 current power level: 1
[*08/16/2023 08:18:25.996692] UP_CFG:4 R1 band 1 set tx power level: 1
[*08/16/2023 08:18:26.003904] UP_DRV:1 R1 WGB uplink mode started
[*08/16/2023 08:18:26.872086] UP_EVT:4 Reset aux scan
```

```
[*08/16/2023 08:18:26.872096] UP_EVT:4 Pause aux scan on slot 2
[*08/16/2023 08:18:26.872100] SC_MST:4 R2 reset uplink scan state to idle
[*08/16/2023 08:18:26.872104] UP_EVT:4 Aux bring down vap - scan
[*08/16/2023 08:18:26.872123] UP_EVT:4 Aux bring up vap - serv
[*08/16/2023 08:18:26.872514] UP_EVT:4 R1 State STOPPED to SCAN_START
[*08/16/2023 08:18:26.8727091 SC_MST:4 R1 Uplink Scan Started.
[*08/16/2023 08:18:26.884054] UP_EVT:8 R1 CH event 149
```

Note It might take a long time to display the **show wgb event** command output in console. Using *ctrl+c* to interrupt the printing will not affect log dump to memory.

The following clear command erases WGB events in memory:

#**clear wgb event** [**basic**|**detail**|**trace**|**all**]

To save all event logs to WGB flash, use the following command:

#**copy event-logging flash**

The package file consists of four separate log files for different log levels.

You can also save event log to a remote server by using the following command:

#**copy event-logging upload** <**tftp** | **sftp** | **scp**>**:**//A.B.C.D[/*dir*][/*filename.tar.gz*]

The following example saves event log to a TFTP server:

```
APC0F8.7FE5.F3C0#copy event-logging upload
tftp://192.168.100.100/tftpuser/evtlog-2023-05-31_11:45:49.tar.gz
Starting upload of WGB config
tftp://192.168.100.100/tftpuser/evtlog-2023-05-31_11:45:49.tar.gz ...
It may take a few seconds. If longer, please cancel command, check network and try again.
########################################################################## 100.0%
Config upload completed.
```

802.11v features

The 802.11v is a wireless network management standard that

- enables network-assisted roaming to optimize client connectivity,
- helps balance client load by providing guidance to client devices, and
- improves wireless performance through enhanced management frames and procedures.

802.11v is part of the IEEE 802.11 family of Wi-Fi standards. It includes features such as network-assisted roaming, which allows network infrastructure (such as wireless controllers) to direct clients to better access points (APs), reducing congestion and improving overall network efficiency.

Enhancement of roaming with 802.11v support

When 802.11v support is enabled on a Workgroup Bridge (WGB), it enhances roaming by enabling the WGB to proactively select optimal APs based on updated neighborhood information:

- The WGB can actively initiate roaming to suitable APs from dynamically updated lists.

- Periodic checks ensure that the WGB maintains the most accurate AP neighbor data, enabling optimal decisions during roaming.

Basic service set transition request frame

The Basic Service Set (BSS) Transition Request frame includes channel information of neighboring APs. Limiting scanning to these specified channels significantly reduces roaming latency in environments that use multiple channels.

Disassociate the client on the AP using WLC

The Wireless LAN Controller (WLC) can disassociate a client based on factors such as AP load, Received Signal Strength Indicator (RSSI), and data rate. Key points include:

- The WLC can notify 802.11v-enabled clients of an impending disassociation through the BSS transition management request frame.
- If the client fails to re-associate with another AP within a configurable time, the disassociation is enforced.

Additional reference information

Administrators can enable the disassociation-imminent configuration on the WLC, which activates the optional field within the BSS transition management request frame.

For detailed information of 802.11v configuration on the WLC, see Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide.

Configure Aux Scanning

The aux-scan mode can be configured as either scanning only or handoff mode on WGB radio 2 (5 GHz) to improve roaming performance. When roaming is triggered, the WGB refers to the scanning table to find the best parent AP. The scanning table is updated using: radio 0 or radio 4 for 2.4 GHz, and radio 1 or radio 4 for 5 GHz.

- Overview of Scanning-Only Mode
- Configuring Scanning Only Mode
- Radio 4 as Scanning Only Mode
- Configuring Aux-Scan Handoff Mode
- Optimized Roaming with Dual-Radio WGB

Scan-only mode

The scanning-only mode is a wireless access point operational mode that:

- enables radio operation exclusively for scanning,
- continuously monitors the wireless environment to collect data on network performance, interference, and rogue devices, and

- allows configuration of scanning parameters such as channel lists and scanning intervals.

When slot 2 radio is configured in scanning-only mode, slot 1 (5G) radio is always selected as the uplink. Slot 2 (5G) radio continues to scan the configured SSID based on the channel list. By default, the channel list contains all supported 5G channels (based on reg domain). You can configure the scanning list manually, or the device can learn it from 802.11v.

When roaming is triggered, the algorithm looks for candidates in the scanning table and skips the scanning phase if the table is not empty. The WGB then associates to the selected candidate AP.

Scanning only mode

When slot 2 radio is configured as scanning only mode, slot 1 (5G) radio will always be picked as uplink. Slot 2 (5G) radio will keep scanning configured SSID based on the channel list. By default, the channel list contains all supported 5G channels (based on reg domain). The scanning list can be configured manually or learned by 802.11v.

When roaming is triggered, the algorithm looks for candidates from scanning table and skips scanning phase if the table is not empty. WGB then makes an assocaition to that candidate AP.

Configure scanning only mode

Use the **configure dot11Radio 2 mode scan only** command to configure scanning only mode.

```
Device#configure dot11Radio 2 mode scan only
```

Manually configure the channel list

Use the **configure wgb mobile station interface dot11Radio 1 scan** <*channel*> **add** command to manually add the channel to the channel list.

```
Device#configure wgb mobile station interface dot11Radio 1 scan <channel> [add|delete]
```

Note Use the **configure wgb mobile station interface dot11Radio 1 scan** <*channel*> **delete** command to manually delete the channel from the channel list.

Configure scanning table timer

Use the **configure wgb scan radio 2 timeout***1500* command to adjust the timer. By default, candidate AP entries in scanning table are automatically removed in 1200 ms.

```
Device#configure wgb scan radio 2 timeout 1500
```

Note

- Scanning AP expire time is from 1 to 5000.
- From the scanning table, the AP selects the candidate with the best RSSI value. However, sometimes the RSSI values might not be updated and it lead to roaming failures.

Verify scanning table

Use **show wgb scan** command to verify the scanning table.

```
Device#show wgb scan
Best AP expire time: 5000 ms

************[ AP List ]***************
BSSID                RSSI   CHANNEL   Time
FC:58:9A:15:E2:4F     84     136       1531
FC:58:9A:15:DE:4F     37     136       41

***********[ Best AP ]****************
BSSID                RSSI   CHANNEL   Time
FC:58:9A:15:DE:4F    37     136       41
```

Radio 4 as Scanning-Only Mode

Before the Cisco IOS-XE 17.15.1 release, only radio 2 (5 GHz) could be configured for scanning purposes. From CiscoIOS-XE 17.15.1 release, radio 4 (in IW9167E AP) can be configured in scanning-only mode.

Radio 4 has the following transmission and reception antennas:

- One transmission antenna for transmitting data from 2.4 GHz and 5 GHz frequency bands.
- Two reception antennas for receiving data from 2.4 GHz, 5 GHz, and 6 GHz frequency bands.

Note When both radio 2 and radio 4 are enabled with the scanning function simultaneously, the WGB uses radio 4 for scanning purpose, and the radio 2 becomes inactive.

Advantages of using Radio 4 as Scanning Only Mode

- The WGB aux scanning and roaming now support both 2.4 GHz and 5 GHz frequencies.
- The antenna resource can be saved because the scanning radio shares its antenna with the serving radio.

Note The roaming performance remains same along with the WGB aux scanning function on radio 2.

Comparision Between Radio 2 or Radio 4 as Scanning Only Mode

Scanning Support	Radio 2 (5 GHz)	Radio 4 (Dedicated Aux Radio)
2.4 GHz	No	Yes
5 GHz	Yes	Yes
Scanning only mode	Yes	Yes
Scan handoff mode	Yes	No

Scanning Support	Radio 2 (5 GHz)	Radio 4 (Dedicated Aux Radio)
Aux-Scan antenna requirement	Additional antennas are required to provide the benefit of RF coverage diversity.	The scanning radio uses the antenna of serving radio.

Connection Map between Dedicated Aux Radio and Serving Radios

Dedicated Aux Radio	Serving Radio
2.4 GHz transmission	Antenna 1
5 GHz transmission	Antenna 4
2.4 GHz reception	Antenna 2 Antenna 3
5 GHz reception	Antenna 3 Antenna 2

Configure Radio 4 as Scanning Only Mode

To configure radio 4 to operate in scanning-only mode, use the command given here:

```
#config wgb aux-radio scan
```

To disable radio 4 for scanning-only mode, use the command given here:

```
#config wgb aux-radio disable
```

Verify Radio 4 Scanning Only Mode Configuration

To verify radio 4 as scanning-only mode, use the command given here:

```
#show running-config
AP Name             : APFC58.9A16.E538
AP Mode             : WorkGroupBridge
CDP State            : Enabled
Watchdog monitoring : Enabled
SSH State            : Enabled
AP Username          : cisco
Session Timeout     : 300
WGB Trace           : Disabled
Syslog Host          : 0.0.0.0
Radio and WLAN-Profile Mapping
===================================
Radio ID    Radio Mode    SSID-Profile       SSID         Authentication
-------------------------------------------------------------------------------
1           WGB           wyj-open           wyj-open     OPEN
2           SCAN          wyj-open           wyj-open     OPEN

Radio Configurations
   .
   .
   .
   Radio Id                    : 2
   Admin state              : ENABLED
   Mode                     : SCAN - Handoff
```

```
   Spatial Stream          : AUTO
   Guard Interval          : 800 ns
   Dot11 type              : 11ax
   11v BSS-Neighbor        : Disabled
   A-MPDU priority         : 0x3f
   A-MPDU subframe number  : 255
   RTS Protection          : 2347(default)
   Rx-SOP Threshold        : AUTO
   Radio profile           : NA
Radio Id                   : 4 (Aux Radio)
   Admin state             : ENABLED
   Mode                    : SCAN
```

The scan result shown with the following show command:

```
#show wgb scan
 Aux Scanning Configure:
 Radio Id: 1
        Admin State: ENABLED
        Mode: WGB
Radio Id: 2
        Admin State: ENABLED
        Mode: SCAN - Handoff
Radio Id: 4 (Aux Radio)
        Admin State: ENABLED
        Mode: SCAN
Best AP expire time: 5000 ms
Aux Scanning State: RUNNING
Aux Scanning Radio Results (Radio 4)
************[ AP List]***************
BSSID                RSSI   CHANNEL   Time
C8:84:A1:D9:B6:8E     35     149       2914

***********[ Best AP]****************
BSSID                RSSI   CHANNEL   Time
C8:84:A1:D9:B6:8E    35     149       2914

Aux Serving Radio Results (Radio1)
************[ AP List]***************
BSSID                RSSI   CHANNEL   Time
C8:84:A1:D0:A3:8E     18     36       4

***********[ Best AP]****************
BSSID                RSSI   CHANNEL   Time
C8:84:A1:D0:A3:8E    18     36       5
```

Configuring Aux-Scan Handoff Mode

When slot 2 radio is configured as handoff mode, both radio 1 and radio 2 are the uplink candidate. While one radio maintains wireless uplink, the other radio keeps scanning the channels. The scanning list can be configured manually or learned by 802.11v.

Radio 2 shares the same MAC address with radio 1, and supports the scanning function, association, and data serving. Both radios can work as **serving** or **scanning** role. When a roaming is triggered, the algorithm looks for the scanning database (internal tables), selects the best candidate AP and makes connection. The radio roles and traffic will dynamically switch between slot 1 and slot 2 after each roaming. WGB always uses the radio with operating role of **scanning** to complete the roaming association to a new AP. With this configuration, the roaming interruption time can be improved to 20-50 ms.

The following table compares roaming interruption time (3 channel case) in various mechanisms:

Roaming Interruption Time	Normal Channel Setting	Aux-scan Only	Aux-scan Handoff
Scanning	(40+20)*3=180 ms	0+40 ms	0 ms
Association	30-80 ms	30-80 ms	20-50 ms
Total	~210 ms	70-120 ms	20-50 ms

Use the following command to configure the WGB slot2 radio to aux-scan mode:

configure dot11Radio 2 mode scan handoff

Use the **show run** command to check your configuration:

```
#show run
...
Radio Id                    : 1
   Admin state              : ENABLED
   Mode                     : WGB
   Spatial Stream           : 1
   Guard Interval           : 800 ns
   Dot11 type               : 11n
   11v BSS-Neighbor         : Disabled
   A-MPDU priority          : 0x3f
   A-MPDU subframe number   : 12
   RTS Protection           : 2347(default)
   Rx-SOP Threshold         : AUTO
   Radio profile            : Default
   Encryption mode          : AES128
Radio Id                    : 2
   Admin state              : ENABLED
   Mode                     : SCAN - Handoff
   Spatial Stream           : 1
   Guard Interval           : 800 ns
   Dot11 type               : 11n
   11v BSS-Neighbor         : Disabled
   A-MPDU priority          : 0x3f
   A-MPDU subframe number   : 12
   RTS Protection           : 2347(default)
   Rx-SOP Threshold         : AUTO
   Radio profile            : Default
```

Use the **show wgb scan** command to display the current role of each radio and the aux scanning results:

```
APFC58.9A15.C808#show wgb scan
Best AP expire time: 2500 ms

Aux Scanning Radio Results (slot 2)
************[ AP List ]***************
BSSID                RSSI   CHANNEL   Time
FC:58:9A:15:DE:4E     54     153       57
FC:58:9A:15:E2:4E     71     153       64

***********[ Best AP ]****************
BSSID                RSSI   CHANNEL   Time
FC:58:9A:15:DE:4E    54     153       57

Aux Serving Radio Results
************[ AP List ]***************
BSSID                RSSI   CHANNEL   Time
FC:58:9A:15:DE:4E     58     153       57
FC:58:9A:15:E2:4E     75     153       133
```

```
***********[ Best AP ]***************
BSSID               RSSI   CHANNEL   Time
FC:58:9A:15:DE:4E   58     153       57
```

Optimized Roaming with Dual-Radio WGB

From the Cisco IOS-XE 17.15.1 release, devices with dual-radio configurations have improved roaming efficiency. Roaming is triggered due to continuous missing beacon frames or maximum packet retries. The second radio allows the WGB to skip the scanning phase and directly check the scanning table for potential APs. This process reduces service downtime.

Trigger Factors for Roaming

Roamingis triggered in these events:

- Low RSSI: Measures the power level that a wireless device, such as an AP, receives from a signal. Use RSSI values to determine the quality of the wireless connection to troubleshoot and optimize wireless networks.
- Beacon miss-count: Indicates the number of consecutive beacon frames that a client device has missed from an AP in a wireless network.
- Maximum packet retries: Specifies the maximum number of times a data packet can be retransmitted if the client device does not send an acknowledgement.

Dual-Radio Configuration

Hereare the possible configurations for the IW9167E AP in a dual-radio setup:

Dual-Radio	AP
2.4 GHz radio 0 + radio 4 (dedicated aux radio)	IW9167E
5 GHz radio 1 + radio 2 (scanning-only mode)	
5 GHz radio 1 + radio 2 (aux-scan handoff mode)	
5 GHz radio 1 + radio 4 (dedicated aux radio)	

Layer 2 NAT

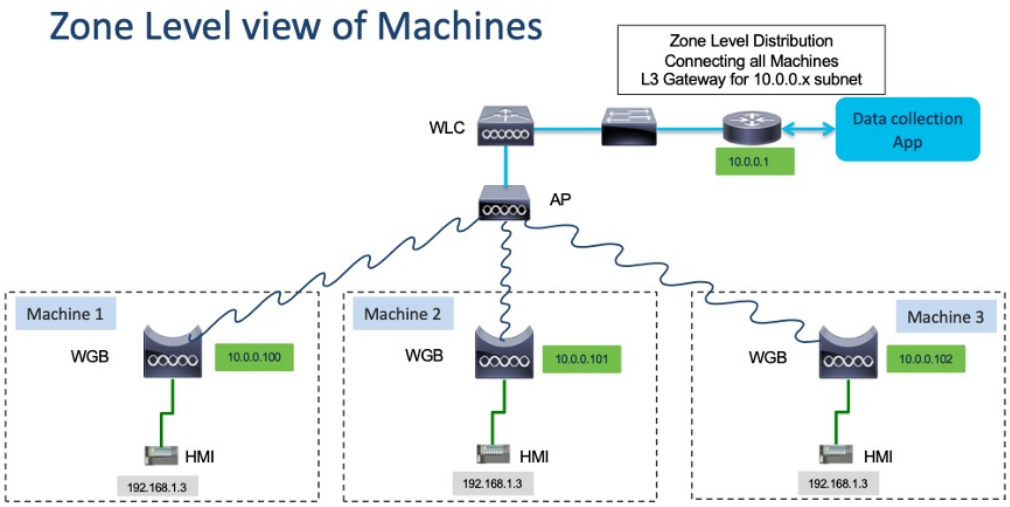
One-to-one (1:1) Layer 2 NAT allows you to assign a unique public IP address to an existing private IP address (end device). This enables the end device to communicate with a public network.

Layer 2 NAT maintains two translation tables:

- private-to-public subnet translations
- public-to-private subnet translations

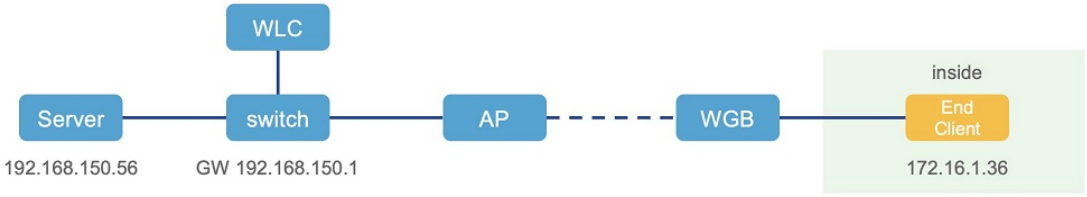
In industrial deployments, such as Human Machine Interfaces (HMIs) or robots, the same firmware is often programmed on every machine. This results in duplicate IP addresses across multiple devices. Layer 2 NAT

resolves this issue by enabling devices with duplicate private IP addresses to communicate with public networks.



Configuration Example of Host IP Address Translation

In this scenario, the end client (172.16.1.36) connected to WGB needs to communicate with the server (192.168.150.56) connected to the gateway. Layer 2 NAT provides an address for the end client on the outside network (192.168.150.36) and an address for the server on the inside network (172.16.1.56).



Layer 2 NAT configuration example

This example displays Layer 2 NAT configuration details. In the output, I2O means 'inside to outside' and O2I means 'outside to inside.

```
Device# show l2nat config

L2NAT Configuration are:
==================================
Status: enabled
Default Vlan: 0
The Number of L2nat Rules: 4
Dir      Inside                    Outside                   Vlan
O2I      172.16.1.56               192.168.150.56            0
I2O      172.16.1.36               192.168.150.36            0
I2O      172.16.1.255              192.168.150.255           0
I2O      172.16.1.1                192.168.150.1             0
```

Layer 2 NAT rules example

This example displays the Layer 2 NAT rules.

```
Device# show l2nat rule

Dir      Inside                  Outside                 Vlan
O2I      172.16.1.56             192.168.150.56          0
I2O      172.16.1.36             192.168.150.36          0
I2O      172.16.1.255            192.168.150.255         0
I2O      172.16.1.1              192.168.150.1           0
```

Layer 2 NAT entries example

This example displays the current Layer 2 NAT entries.

```
Device# show l2nat entry

Direction            Original            Substitute             Age    Reversed
inside-to-outside    172.16.1.36@0       192.168.150. 36@0      -1     false
inside-to-outside    172.16.1.56@0       192.168.150. 56@0      -1     true
inside-to-outside    172.16.1.1@0        192.168.150. 1@0       -1     false
inside-to-outside    172.16.1.255@0      192.168.150. 255@0     -1     false
outside-to-inside    192.168.150.36@0    172.16.1.36@0          -1     true
outside-to-inside    192.168.150.56@0    172.16.1.56@0          -1     false
outside-to-inside    192.168.150.1@0     172.16.1.1@0           -1     true
outside-to-inside    192.168.150.255@0   172.16.1.255@0         -1     true
```

WGB wired clients example

This example displays the WGB wired clients over the bridge.

Before Layer 2 NAT is enabled:

```
Device# show wgb bridge
    ***Client ip table entries***
              mac vap     port vlan_id          seen_ip  confirm_ago  fast_brg
B8:AE:ED:7E:46:EB   0   wired0       0      172.16.1.36     0.360000      true
24:16:1B:F8:05:0F   0 wbridge1       0          0.0.0.0  3420.560000      true
```

After Layer 2 NAT is enabled:

```
Device# show wgb bridge
    ***Client ip table entries***
              mac vap     port vlan_id          seen_ip  confirm_ago  fast_brg
B8:AE:ED:7E:46:EB   0   wired0       0   192.168.150.36     0.440000      true
24:16:1B:F8:05:0F   0 wbridge1       0          0.0.0.0  3502.220000      true
```



Note If the wired client in NAT experiences E2E traffic issues, you can restart the client registration process by using the **clear wgb client single** command:

Layer 2 NAT packet translation statistics example

This example displays the Layer 2 NAT packet translation statistics.

```
Device# show l2nat stats

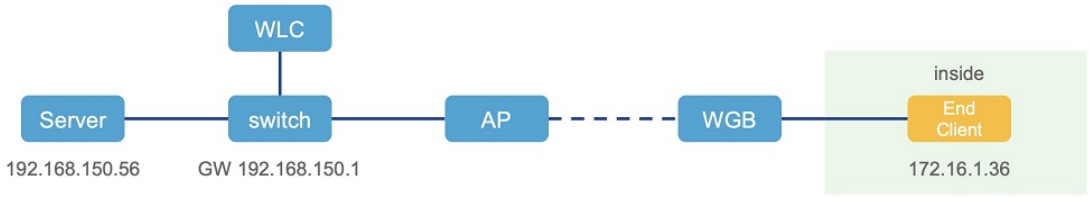
Direction          Original              Substitute            ARP  IP   ICMP UDP  TCP
inside-to-outside  172.16.1.1@2660       192.168.150.1@2660    1    4    4    0    0
inside-to-outside  172.16.1.36@2660      192.168.150.36@2660   3    129  32   90   1
```

```
inside-to-outside  172.16.1.56@2660      192.168.150.56@2660   2    114  28   85   1
inside-to-outside  172.16.1.255@2660     192.168.150.255@2660  0    0    0    0    0
outside-to-inside  192.168.150.1@2660    172.16.1.1@2660       1    4    4    0    0
outside-to-inside  192.168.150.36@2660   172.16.1.36@2660      3    39   38   0    1
outside-to-inside  192.168.150.56@2660   172.16.1.56@2660      2    35   34   0    1
outside-to-inside  192.168.150.255@2660  172.16.1.255@2660     0    0    0    0    0
```

Note To reset the statistics, you can use the **clear l2nat stats** command.

Configuration Example of Network Address Translation

In this scenario, Layer 2 NAT translates inside addresses in the 172.16.1.0/24 subnet to addresses in the 192.168.150.0/24 subnet, replacing only the network prefix during translation. The host bits remain the same.



The command used for this scenario is here:

```
Device# configure l2nat add inside from network 172.16.1.0 to 192.168.150.0 255.255.255.0
```

Native VLAN on Ethernet Ports

In a typical Workgroup Bridge (WGB) deployment, a single wired client connects directly to the WGB Ethernet port. Consequently, the wired client traffic must reside on the same VLAN as the WGB management VLAN. If you require the wired client traffic to be on a different VLAN than the WGB management VLAN, configure the native VLAN on the Ethernet port.

Important Configuring native VLAN ID per Ethernet port is not supported. Both Ethernet ports share the same native VLAN configuration.

Caution When WGB broadcast tagging is enabled and a single wired passive client connects directly to the WGB Ethernet port, an issue may arise where the infrastructure downstream (DS) side client fails to ping the WGB behind the passive client. To resolve this, configure the following commands: `configure wgb ethport native-vlan enable` and **configure wgb ethport native-vlan id X**, where X is the same VLAN as the WGB management VLAN.

To verify your configuration, use the **show wgb ethport config** or **show running-config** command.

Low latency profile

Low latency profiles are configurations that optimize IEEE 802.11 networks to meet the low latency and Quality of Service (QoS) requirements essential for IoT applications. IEEE 802.11 networks play a vital role in enabling IoT applications by providing mechanisms that reduce latency and ensure QoS. The following features are key to achieving these goals:

- Enhanced Distributed Channel Access (EDCA): EDCA parameters prioritize wireless channel access for latency-sensitive traffic, such as voice and video streams, ensuring consistent QoS performance.
- Aggregated MAC Protocol Data Unit (AMPDU): This mechanism combines multiple data frames into a single transmission, reducing overhead and improving efficiency.
- Packet Retry (Aggregated or Non-Aggregated): The retry mechanism ensures successful data delivery, either by retransmitting aggregated packets or individual packets, depending on network conditions.

These features collectively support the deployment of IoT devices and applications that demand low latency and high QoS in wireless environments.

Configuring WGB optimized-video EDCA Profile

To configure optimized low latency profile for video use case, use the following command:

#**configure dot11Radio** <*radio_slot_id*> **profile optimized-video** {**enable** | **disable**}

Use the following command to verify the configuration:

```
WGB1#show controllers dot11Radio 1
EDCA profile: optimized-video
EDCA in use
=============
AC Type CwMin CwMax Aifs Txop ACM
AC_BE L 4 10 11 0 0
AC_BK L 6 10 11 0 0
AC_VI L 3 4 2 94 0
AC_VO L 2 3 1 47 0

Packet parameters in use
=============
wbridge1 A-MPDU Priority 0: Enabled
wbridge1 A-MPDU Priority 1: Enabled
wbridge1 A-MPDU Priority 2: Enabled
wbridge1 A-MPDU Priority 3: Enabled
wbridge1 A-MPDU Priority 4: Disabled
wbridge1 A-MPDU Priority 5: Disabled
wbridge1 A-MPDU Priority 6: Disabled
wbridge1 A-MPDU Priority 7: Disabled
wbridge1 A-MPDU subframe number: 3
wbridge1 Packet retries drop threshold: 16
```

Configuring WGB optimized-automation EDCA Profile

To configure optimized low latency profile for automation use case, use the following command:

#**configure dot11Radio** <*radio_slot_id*> **profile optimized-automation** {**enable** | **disable**}

Use the following command to verify the configuration:

```
WGB1#show controllers dot11Radio 1
EDCA profile: optimized-automation
EDCA in use
=============
AC Type CwMin CwMax Aifs Txop ACM
AC_BE L 7 10 12 0 0
AC_BK L 8 10 12 0 0
AC_VI L 7 7 3 0 0
AC_VO L 3 3 1 0 0

Packet parameters in use
=============
wbridge1 A-MPDU Priority 0: Enabled
wbridge1 A-MPDU Priority 1: Enabled
wbridge1 A-MPDU Priority 2: Enabled
wbridge1 A-MPDU Priority 3: Enabled
wbridge1 A-MPDU Priority 4: Disabled
wbridge1 A-MPDU Priority 5: Disabled
wbridge1 A-MPDU Priority 6: Disabled
wbridge1 A-MPDU Priority 7: Disabled
wbridge1 A-MPDU subframe number: 3
wbridge1 Packet retries drop threshold: 16
```

Configuring WGB customized-wmm EDCA profile

To configure customized Wi-Fi Multimedia (WMM) profile, use the following command:

#**configure dot11Radio** <*radio_slot_id*> **profile customized-wmm** {**enable** | **disable**}

To configure customized WMM profile parameters, use the following command:

#**configure dot11Radio** {**0**|**1**|**2**} **wmm** {**be** | **vi** | **vo** | **bk**} {**cwmin** <*cwmin_num*> | **cwmax** <*cwmax_num*> | **aifs** <*aifs_num*> | **txoplimit** <*txoplimit_num*>}

Parameter descriptions:

- be—best-effort traffic queue (CS0 and CS3)
- bk—background traffic queue (CS1 and CS2)
- vi—video traffic queue (CS4 and CS5)
- vo—voice traffic queue (CS6 and CS7)
- aifs—Arbitration Inter-Frame Spacing, <1-15> in units of slot time
- cwmin—Contention Window min, <0-15> 2^n-1, in units of slot time
- cwmax—Contention Window max, <0-15> 2^n-1, in units of slot time
- txoplimit—Transmission opportunity time, <0-255> integer number, in units of 32us

Configuring Low Latency Profile on WGB

Use the following command to configure low latency profile on WGB:

AP# **configure dot11Radio** <*radio_slot_id*> **profile low-latency** [**ampdu** <*length*>] [**sifs-burst** {**enable** | **disable**}] [**rts-cts** {**enable** | **disable**}] [**non-aggr** <*length*>] [**aggr** <*length*>]

Use the following command to display iot-low-latency profile EDCA detailed parameters:

```
#show controllers dot11Radio 1 | beg EDCA
EDCA config
L: Local C:Cell A:Adaptive EDCA params
  AC    Type  CwMin  CwMax Aifs Txop ACM
AC_BE     L      4      6   11    0   0
AC_BK     L      6     10   11    0   0
AC_VI     L      3      4    1    0   0
AC_VO     L      0      2    0    0   1
AC_BE     C      4     10   11    0   0
AC_BK     C      6     10   11    0   0
AC_VI     C      3      4    2   94   0
AC_VO     C      2      3    1   47   1
```

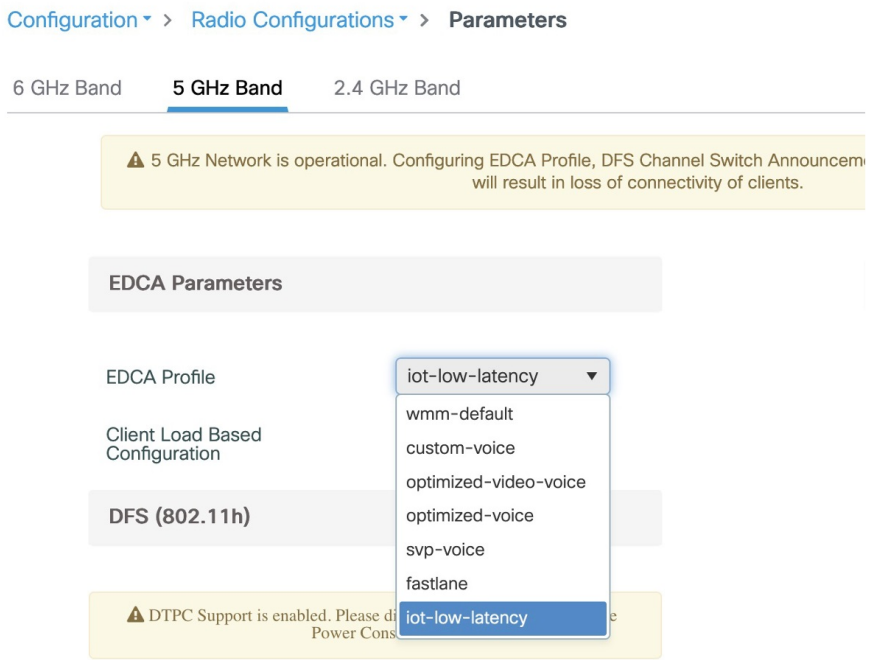
Configure EDCA parameters using Controller GUI

Procedure

Step 1 Choose **Configuration > Radio Configurations > Parameters**. Using this page, you can configure global parameters for 6 GHz, 5 GHz, and 2.4 GHz radios.

Note
You cannot configure or modify parameters, if the radio network is enabled. Disable the network status on the **Configuration > Radio Configurations > Network** page before you proceed.

Step 2 In the **EDCA Parameters** section, choose an EDCA profile from the **EDCA Profile** drop-down list. Enhanced Distributed Channel Access (EDCA) parameters are designed to provide preferential wireless channel access for voice, video, and other quality-of-service (QoS) traffic.



Step 3 Click **Apply**.

Configuring EDCA Parameters (Wireless Controller CLI)

Procedure

Step 1 Enters global configuration mode.

configure terminal

Example:

```
Device# configure terminal
```

Step 2 Disables the radio network.

ap dot11 {**5ghz** | **24ghz** | **6ghz**} **shutdown**

Example:

```
Device(config)# ap dot11 5ghz shutdown
```

Step 3 Enables iot-low-latency EDCA profile for the 5 GHz, 2.4 GHz, or 6 GHz network.

ap dot11 {**5ghz** | **24ghz** | **6ghz**} **edca-parameters iot-low-latency**

Example:

```
Device(config)# ap dot11 5ghz edca-parameters iot-low-latency
```

Step 4 Enables the radio network.

no ap dot11 {**5ghz** | **24ghz** | **6ghz**} **shutdown**

Example:

```
Device(config)# no ap dot11 5ghz shutdown
```

Step 5 Returns to privileged EXEC mode.

end

Example:

```
Device(config)# end
```

Step 6 Displays the current configuration.

show ap dot11 {**5ghz** | **24ghz** | **6ghz**} **network**

Example:

```
Device(config)# show ap dot11 5ghz network
EDCA profile type check                  : iot-low-latency
```

Configuring A-MPDU

Aggregation is the process of grouping packet data frames together, rather than transmitting them separately. Two aggregation methods are available: Aggregated MAC Protocol Data Unit (A-MPDU) and Aggregated MAC Service Data Unit (A-MSDU).

The A-MPDU parameters define the size of an aggregated packet and define the proper spacing between aggregated packets so that the receive side WLAN station can decode the packet properly.

To configure profiled based A-MPDU under 2.4G, 5G and 6G radio, use the following commands:

WLC(config)# **ap dot11** {**5ghz** | **24ghz** | **6ghz**} **rf-profile** <*profile-name*>

WLC(config-rf-profile)# [**no**] **dot11n a-mpdu tx block-ack window-size** <*1-255*>

Global configuration is a special profile which can also be configured bu using the following command:

WLC(config)#[**no**] **ap dot11** {**5ghz** | **24ghz** | **6ghz**} **dot11n a-mpdu tx block-ack window-size** <*1-255*>

To bind different RF profiles with the radio RF tag, use the following command:

WLC(config)# **wireless tag rf** <*rf-tag-name*>

WLC (config-wireless-rf-tag)# **5ghz-rf-policy** <*rf-profile-name*>

Note RF profile level configured **a-mpdu tx block-ack window-size** value takes preference over globally configured value.

To display configured a-mpdu length value, use the following command:

show controllers dot11Radio <*radio_slot_id*>

```
AP# show controllers dot11Radio 1
Radio Aggregation Config:
=========================

TX A-MPDU Priority: 0x3f
TX A-MSDU Priority: 0x3f
TX A-MPDU Window:   0x7f
```

Configuring WGB/uWGB Radio Parameters

Configuring WGB Radio Antenna

Use the following command to configure WGB radio antenna gain. The default antenna gain is 4 dBi.

configure dot11 <**0|1|2**> **antenna gain** <*1-30*>

Use the following command to configure WGB radio antenna. Default is abcd-antenna.

configure dot11 <**0|1|2**> **antenna** <**a-antenna**|**ab-antenna**|**abcd-antenna**>

802.11ax 1600ns and 3200ns Guard Interval

802.11ax supports multiple Guard Interval (GI) value: 800ns, 1600ns, and 3200ns. By default, GI is set to 800ns. But you can set it to a different value.

Longer GI is commonly used in outdoor deployment.

```
#configure dot11radio <0|1|2> guard-interval
  1600  Configure 1600 ns guard interval (only in HE mode)
  3200  Configure 3200 ns guard interval (only in HE mode)
  800   Configure 800 ns guard interval
```

Customized Transmit Power

By default, the transmit power of the radio is set to AUTO(0) level.

To manually set the transmit power of the radio use the following command:

```
# configure Dot11Radio <0|1|2> txpower-level <0-8>
```

Assign Country Code to WGB/uWGB With -ROW PID

On day 0, you should assign proper country code to the WGB/uWGB with -ROW reg domain. WGB will load corresponding power table after rebooting.

To assign country code, use the following command:

```
#configure countrycode
  Supported ROW country codes:
  GB VN

  WORD  Select one of above ROW country codes.
```

Note After the ROW country code is configured, if you want to change the configuration to another country, you need to perform a factory reset first, and then configure the new country code.

Indoor Deployment for -E Domain and United Kingdom

IW9167EH supports indoor deployment for -E domain and GB in -ROW domain .

For outdoor mode, the IW9167EH 5G radio supports channels 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140. When indoor deployment is enabled, 5G radio supports channels 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140.

To configure indoor mode, use the **configure wireless indoor-deployment enable** command.

To disable indoor mode, use the **configure wireless indoor-deployment disable** command.

```
#configure wireless indoor-deployment
  disable  Disable indoor deployment
  enable   Enable indoor deployment
```

You can check the indoor or outdoor mode by using the **show controllers Dot11Radio [1|2]** command. In the command output, "-Ei" means the indoor mode is enabled, and "-E" means indoor mode is disabled, as shown in the following examples. The CLI output also shows the supported channels.

```
#show controllers Dot11Radio [1|2]
…
Radio Info Summary:
=======================
Radio: 5.0GHz
Carrier Set: (-Ei)  ( GB )
Base radio MAC: FC:58:9A:15:B7:C0
Supported Channels:
36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140

#show controllers Dot11Radio [1|2]
…
Radio Info Summary:
=======================
Radio: 5.0GHz
Carrier Set: (-E)  ( GB )
Base radio MAC: FC:58:9A:15:B7:C0
Supported Channels:
100 104 108 112 116 120 124 128 132 136 140
```

Configuring WGB Roaming Parameters

Use the following command to configure the threshold duration and signal strength to trigger reconnecting. Default value is: period 20s and threshold -70db.

```
# configure wgb mobile period <time> <rssi-threshold>
```

Use the following command to configure beacon miss count to trigger reconnecting. Default value is 10.

```
# config wgb beacon miss-count <count>
```

Use the following command to configure max packet retry to trigger reconnecting. Default value is 64.

```
# configure wgb packet retries <retry-count>
```

Use the following command to configure the static roaming channel:

```
# configure wgb mobile station interface dot11Radio <slot_id> scan <channel_id> add
```

Use the following command to delete the mobile channel:

```
# configure wgb mobile station interface dot11Radio <slot_id> scan <channel_id> delete
```

Use the following command to scan all channels:

```
# configure wgb mobile station interface Dot11Radio 1 scan all
```

Importing and Exporting WGB Configuration

You can upload the working configuration of an existing WGB to a server, and then download it to the new deployed WGBs.

To upload the configuration to a server, use the following command:

```
#copy configuration upload <sftp:|tftp://> ip-address [directory] [file-name]
```

To download a sample configuration to all WGBs in the deployment, use the following command:

```
#copy configuration download <sftp:|tftp://> ip-address [directory] [file-name]
```

The access point will reboot after the **copy configuration download** command is executed. The imported configuration will take effect after the rebooting.

Verifying the Configuration of WGB and uWGB

Use the **show run** command to check whether the AP is in WGB mode or uWGB mode.

- WGB:

```
#show run
AP Name              : APFC58.9A15.C808
AP Mode              : WorkGroupBridge
CDP State            : Enabled
Watchdog monitoring  : Enabled
SSH State            : Disabled
AP Username          : admin
Session Timeout      : 300


Radio and WLAN-Profile mapping:-
===================================
Radio ID    Radio Mode    SSID-Profile                    SSID
          Authentication
-------------------------------------------------------------------------------
--------------------------
1           WGB           myssid                          demo
          OPEN


Radio configurations:-
==============================
Radio Id             : NA
   Admin state       : NA
   Mode              : NA
Radio Id             : 1
   Admin state       : DISABLED
   Mode              : WGB
   Dot11 type        : 11ax
Radio Id             : NA
   Admin state       : NA
   Mode              : NA
```

- uWGB:

```
#show run
AP Name              : APFC58.9A15.C808
AP Mode              : WorkGroupBridge
CDP State            : Enabled
Watchdog monitoring  : Enabled
SSH State            : Disabled
AP Username          : admin
Session Timeout      : 300


Radio and WLAN-Profile mapping:-
===================================
Radio ID    Radio Mode    SSID-Profile                    SSID
          Authentication
-------------------------------------------------------------------------------
```

```
-------------------------
1           UWGB          myssid                          demo
          OPEN


Radio configurations:-
==============================
Radio Id             : NA
   Admin state       : NA
   Mode              : NA
Radio Id             : 1
   Admin state       : DISABLED
   Mode              : UWGB
   Uclient mac       : 0009.0001.0001
   Current state     : WGB
   UClient timeout   : 0 Sec
   Dot11 type        : 11ax
Radio Id             : NA
   Admin state       : NA
   Mode              : NA
```

Use the **show wgb dot11 associations** command to verify the configuration of WGB and uWGB.

- WGB:

```
#show wgb dot11 associations
Uplink Radio ID : 1
Uplink Radio MAC : 00:99:9A:15:B4:91
SSID Name : roam-m44-open
Parent AP Name : APFC58.9A15.C964
Parent AP MAC : 00:99:9A:15:DE:4C
Uplink State : CONNECTED
Auth Type : OPEN
Dot11 type : 11ax
Channel : 100
Bandwidth : 20 MHz
Current Datarate (Tx/Rx) : 86/86 Mbps
Max Datarate : 143 Mbps
RSSI : 53
IP : 192.168.1.101/24
Default Gateway : 192.168.1.1
IPV6 : ::/128
Assoc timeout : 100 Msec
Auth timeout : 100 Msec
Dhcp timeout : 60 Sec
```

- uWGB:

```
#show wgb dot11 associations
Uplink Radio ID : 1
Uplink Radio MAC : 00:09:00:01:00:01
SSID Name : roam-m44-open
Parent AP MAC : FC:58:9A:15:DE:4C
Uplink State : CONNECTED
Auth Type : OPEN
Uclient mac : 00:09:00:01:00:01
Current state : UWGB
Uclient timeout : 60 Sec
Dot11 type : 11ax
Channel : 36
Bandwidth : 20 MHz
Current Datarate (Tx/Rx) : 77/0 Mbps
Max Datarate : 143 Mbps
RSSI : 60
IP : 0.0.0.0
```

```
IPV6 : ::/128
Assoc timeout : 100 Msec
Auth timeout : 100 Msec
Dhcp timeout : 60 Sec
```

SNMP features

The Simple Network Management Protocol (SNMP) on WGB is a functional element that

- facilitates monitoring and management of the WGB device through the SNMP protocol,
- includes roles for information exchange (manager, agent, MIB), and
- supports network health assessment and parameter configuration.

The SNMP framework on WGB includes:

- SNMP Manager: Controls and monitors the activities of network devices using SNMP, typically implemented as a network management system (NMS).
- SNMP Agent: The software component within the managed device that maintains and reports device data.
- SNMP MIB: A collection of managed objects (variables) which can be queried or set by the SNMP manager.

SNMP process

This illustration shows the SNMP process. When an SNMP manager requests data, the agent receives the request and relays it to the subagent, which responds. The agent then sends an SNMP response packet to the manager.

Figure 4: SNMP Process



SNMP versions

Cisco IOS software supports the following versions of SNMP:

- SNMPv2c—The community-string-based administrative framework for SNMPv2. SNMPv2c is an update of the protocol operations and data types of SNMPv2p (SNMPv2 classic), and uses the community-based security model of SNMPv1.
- SNMPv3—Version 3 of SNMP. SNMPv3 uses the following security features to provide secure access to devices:
  - Message integrity—Ensuring that a packet has not been tampered with in transit.
  - Authentication—Determining that the message is from a valid source.
  - Encryption—Scrambling the contents of a packet to prevent it from being learned by an unauthorized source.

Supported SNMP MIB files

The Management Information Base (MIB) is a database containing objects that can be managed on a device. These managed objects, also called variables, can be set or read to provide information about network devices and interfaces. The objects are organized in a hierarchical structure and are grouped in collections identified by object identifiers. Access to MIBs is provided through network management protocols such as SNMP.

The MIB module provides network management information on IEEE 802.11 wireless device association management and data packet forwarding configuration and statistics.

An Object Identifier (OID) uniquely identifies a MIB object on a managed network device. The OID shows the object's location in the MIB hierarchy and provides a way to access the MIB object in a network of managed devices.

Configure SNMP parameters

This procedure describes how to configure Simple Network Management Protocol (SNMP) on the WGB. You can enable SNMPv2c or SNMPv3 depending on your network requirements. The steps include setting community strings or usernames, defining authentication and encryption methods, and enabling SNMP functionality on the device.

- Configure all SNMP parameters before enabling the SNMP feature using the CLI command: **configure snmp enabled**.
- All SNMP configurations will be automatically removed when the SNMP feature is disabled.

Procedure

Step 1 Use the **configure snmp v2c community-id length** *length* command to enter the SNMP v2c community ID (SNMP v2c only).

```
Device#configure snmp v2c community-id 50
```

Step 2 Use the **configure snmp version** {**v2c** | **v3**} command to specify the SNMP protocol version.

```
Device# configure snmp version v3
```

Step 3 Use the **configure snmp auth-method** {**md5** | **sha**} command to specify the SNMP v3 authentication protocol (SNMP v3 only).

```
Device# configure snmp auth-method md5
```

Step 4 Use the **configure snmp v3 username length** *length* command to enter the SNMP v3 username (SNMP v3 only).

```
Device# configure snmp v3 username length 32
```

Step 5 Use the **configure snmp v3 password length** *length* command to enter the SNMP v3 user password (SNMP v3 only).

```
Device# configure snmp v3 password length 12
```

The valid range for *length* is 8 to 64 characters.

Step 6 Use the **configure snmp encryption** {**des** | **aes** | **none**} command to specify the SNMP v3 encryption protocol (SNMP v3 only).

```
Device#configure snmp encryption des
```

Encryption values are **des** or **aes**. Use **none** if a v3 encryption protocol is not needed.

Step 7 Use the **configure snmp secret length** *length* command to enter the SNMP v3 encryption passphrase (SNMP v3 only).

```
Device#configure snmp secret length 12
```

The valid range for *length* is 8 to 64 characters.

Step 8 Use the **configure snmp enabled** command to enable SNMP functionality on the WGB.

```
Device#configure snmp enabled
```

To configure SNMP **v2c**, repeat Step 1, Step 2 and Step 8.

To configure SNMP **v3**, repeat Step 2 through Step 8.

Step 9 (Optional) Use the **configure snmp disabled** command to disable SNMP configuration.

```
Device# configure snmp disabled
```

Verifying SNMP

Use the **show snmp** command to verify the SNMP configuration.

SNMP version v3

```
Device# show snmp

SNMP: enabled
Version: v3
Community ID: test
Username: username
Password: password
Authentication method: SHA
Encryption: AES
Encryption Passphrase: passphrase
Engine ID: 0x8000000903c0f87fe5f314
```

SNMP version v2c

```
Device# show snmp

SNMP: enabled
Version: v2c
Community ID: test
Username: username
Password: password
Authentication method: SHA
Encryption: AES
Encryption Passphrase: passphrase
Engine ID: 0x8000000903c0f87fe5f314
```

QoS ACL classification and marking

Quality of Service (QoS) ACL classification and marking identify network traffic using access control list (ACL) rules and assign a traffic class or priority value.

- Classification uses ACLs to match traffic flows based on parameters such as source or destination IP address, protocol type, port numbers, or other header fields. This step identifies the type of traffic being forwarded, such as voice, video, or data.
- Marking occurs after classification. Packets are tagged with specific QoS values, such as DSCP, IP precedence, or CoS, which indicate their priority level. These markings guide QoS policies such as queuing, policing, or shaping across the network..

Starting with Cisco Unified Industrial Wireless Software Release 17.14.1, you can classify packets from two wired ports and assign them to different access control driver queues based on your configuration.

In addition to TCP and UDP, the WGB supports ethertype-based and DSCP-based classification. The WGB classifies packets and assigns them to access control queues according to the field environment to meet jitter and latency requirements.

Rule-based traffic classifications

A rule-based traffic classification is a network management technique that:

- uses custom rules to classify incoming Ethernet packets by criteria such as 802.1p, DSCP, and protocol type,
- assigns classified packets to priority queues on the wireless side for QoS enforcement, and
- ensures critical services receive higher priority, reducing latency and optimizing network performance.

Rule configuration criteria

You can configure mapping rules using the following parameters:

- Ethernet type (for example, Profinet)
- Transport layer port numbers or port ranges
- DSCP values
- Source and destination IP addresses
- Protocol types

Packet classification and assignment

As incoming packets arrive at the Ethernet port, WGB applies the defined rules to:

- Identify critical services or traffic flows
- Classify packets based on predefined criteria
- Assign packets to the appropriate access control queues on the wireless network

Benefits of rule-based mapping

By using customized rule-based classification and mapping, you can:

- Enforce QoS policies effectively

- Prioritize critical applications and services
- Reduce latency for time-sensitive traffic
- Improve overall network performance and user experience

QoS and ACL traffic classification methods

Traffic classification is the process of distinguishing one type of network traffic from another by examining packet fields. It is enabled only when QoS is active. During classification, the device performs a lookup and assigns a QoS label to the packet. The QoS label defines the QoS actions to be applied and identifies the output queue for forwarding.

- Classification relies on fields across packet layers
- Packets are grouped into service classes based on Ethertype, DSCP, or TCP/UDP ports, and consistently treated within those classes.
- The data plane records rule hits for analysis, while the control plane configures data forwarding.

Layer 2 classification fields

Layer 2 Ethernet frames use the Ethertype field (2 bytes) to carry classification information. This field normally indicates the type of data encapsulated in the frames.

Layer 3 classification fields

Layer 3 IP packets carry classification information in the Type of Service (ToS) field (8 bits). It has:

- IP precedence values that range from 0–7, and
- DSCP values that range from 0–63.

Layer 4 classification fields

Layer 4 TCP segments or UDP datagrams use the source or destination port fields for classification. These port numbers allow devices to classify traffic based on applications or services.

Traffic assignment to service classes

The system assigns traffic to a specific service class based on Ethertype, DSCP, or UDP/TCP port (or port range). Packets within a service class are treated consistently. WGBs classify packets from wired ports and map them to different driver queues according to user configuration.

Data plane role in classification

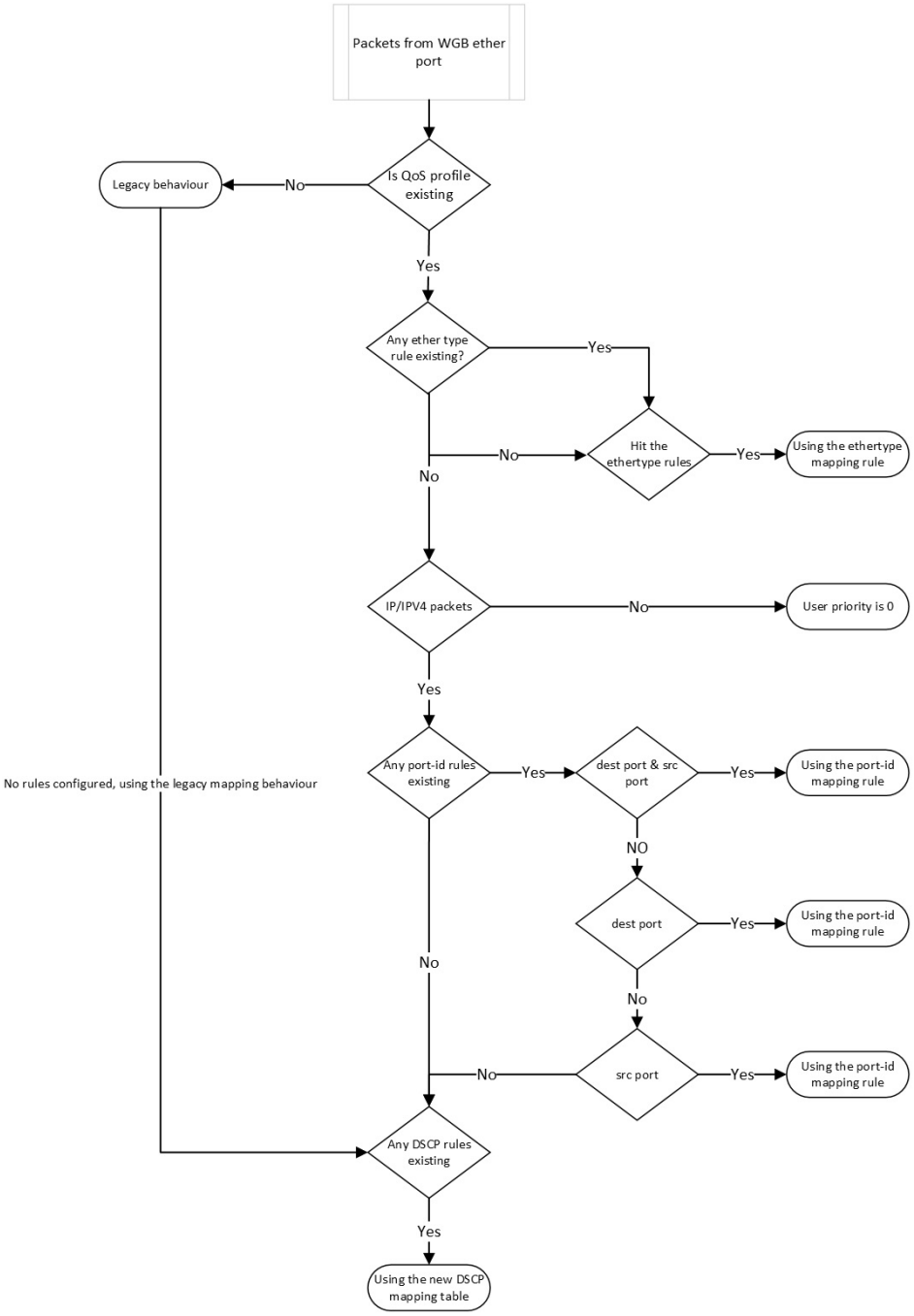
Data plane statistics provide counters showing how many times each rule is matched by traffic. These counters help administrators analyze rule effectiveness and optimize performance.

Control plane role in classification

The control plane is responsible for managing and configuring how data is forwarded through the network.

The following flowchart illustrates how packets from a WGB Ethernet port are classified and mapped to QoS rules based on existing profiles, Ethertype, port identifiers, and DSCP values.

Figure 5: Flowchart of traffic flows from WGB ethernet port



Configure QoS Mapping Profile

This procedure allows you to define the different classification rules for configuring WGB QoS mapping.

Procedure

Step 1 Use the **config wgb qos-mapping** *profile-name* **enable** command to enable the specified QoS mapping profile.

```
Device# configure wgb qos-mapping demo-profile enable
```

Step 2 Use the **config wgb qos-mapping** *profile-name* **add ethtype hex** *hex-number* **priority** *priority* command to add a mapping rule based on Ethernet type.

```
Device# configure wgb qos-mapping demo-profile add ethtype hex 8892 priority 5
```

Note
If the specified profile does not exist, the command creates a new empty profile and adds the mapping rule to it.

You can delete the rules based on ethernet type using the **config wgb qos-mapping** *profile-name* **delete ethtype hex** *hex-number*

Note
If the specified profile does not exist, the command displays a warning. If deleting the mapping rule leaves the profile empty, the profile is automatically removed.

Step 3 Use the **config wgb qos-mapping** *profile-name* **add** [**srcport** *number* | **dstport** *number* | **range** *start-number ending-number*] **priority** *priority* command to add a mapping rule based on port ID or range.

```
Device# config wgb qos-mapping voice-profile add dstport 5004 priority 6
```

Note
If the specified profile does not exist, the command creates a new empty profile and adds the mapping rule.

You can delete rules based on port-id/range using the **config wgb qos-mapping** *profile-name* **delete** [**srcport** *number* | **range** *start-number ending-number* [**dstport** *number* | **range** *start-number ending-number*]]

Note
If the specified profile does not exist, the command displays a warning. If deleting the mapping rule leaves the profile empty, the profile is automatically removed.

Step 4 Use the **config wgb qos-mapping** *profile-name* **add dscp** *number* **priority** *priority* command to add a mapping rule based on DSCP value.

```
Device# configure wgb qos-mapping demo-profile add dscp 63 priority 4
```

Note
If the specified profile does not exist, the command creates a new empty profile and adds the mapping rule.

You can delete a mapping rule based on DSCP value using the **config wgb qos-mapping** *profile-name* **delete dscp** *number* **priority** *priority* command.

Note
If the specified profile does not exist, the command displays a warning. If deleting the mapping rule leaves the profile empty, the profile is automatically removed.

After deleting the DSCP mapping rule, the rules are reset to the default values of the DSCP mapping.

Step 5 Use the **config wgb qos-mapping** *profile-name* **disable** command to disable the specified QoS mapping profile.

```
Device# configure wgb qos-mapping demo-profile disable
```

When disabled, the profile is cleared from the datapath but retained in the WGB configuration file. If the profile does not exist, a warning is issued and no new profile is created.

Step 6 (Optional) Use the **config wgb qos-mapping** *profile-name* **delete** command to delete the specified QoS mapping profile.

```
Device# configure wgb qos-mapping demo-profile delete
```

When deleted, the profile is removed from both the datapath and the WGB configuration.

Verify Quality of Service Map

To verify the QoS mapping configuration on the Control Plane, run the **show wgb qos-mapping**.

```
Device# show wgb qos-mapping

Number of QoS Mapping Profiles: 2
====================================
Profile name : qos1
Profile status : active
Number of Rules: 8
Rules:
L4 srcport : 31000-31100, dstport : 6666-7777, priority : 7
L4 srcport : 23000, dstport : N/A, priority : 3
L4 srcport : N/A, dstport : 20000-20100, priority : 5
L4 srcport : N/A, dstport : 2222, priority : 2
L4 srcport : 12300-12500, dstport : N/A, priority : 6
IPv4/IPv6 dscp: 43, priority : 1
Ethernet type : 0x8892, priority : 0
L4 srcport : 8888, dstport : 9999, priority : 4

Profile name : qos2
Profile status : inactive
Number of Rules: 8
Rules:
L4 srcport : 31000-31100, dstport : 6666-7777, priority : 2
L4 srcport : 23000, dstport : N/A, priority : 6
L4 srcport : N/A, dstport : 20000-20100, priority : 4
L4 srcport : N/A, dstport : 2222, priority : 7
L4 srcport : 12300-12500, dstport : N/A, priority : 3
IPv4/IPv6 dscp: 43, priority : 0
Ethernet type : 0x8892, priority : 1
L4 srcport : 8888, dstport : 9999, priority : 5
```

To verify the WGB QoS mapping configuration on the Data Plane, run the **show datapath qos-mapping rule**.

```
Device# show datapath qos-mapping rule

Status: active
QoS Mapping entries
======= dscp mapping =======
Default dscp2dot1p Table Value:
[0]->0 [1]->0 [2]->0 [3]->0 [4]->0 [5]->0 [6]->0 [7]->0
[8]->1 [9]->1 [10]->1 [11]->1 [12]->1 [13]->1 [14]->1 [15]->1
[16]->2 [17]->2 [18]->2 [19]->2 [20]->2 [21]->2 [22]->2 [23]->2
[24]->3 [25]->3 [26]->3 [27]->3 [28]->3 [29]->3 [30]->3 [31]->3
[32]->4 [33]->4 [34]->4 [35]->4 [36]->4 [37]->4 [38]->4 [39]->4
```

```
[40]->5 [41]->5 [42]->5 [43]->5 [44]->5 [45]->5 [46]->5 [47]->5
[48]->6 [49]->6 [50]->6 [51]->6 [52]->6 [53]->6 [54]->6 [55]->6
[56]->7 [57]->7 [58]->7 [59]->7 [60]->7 [61]->7 [62]->7 [63]->7

active dscp2dot1p Table Value:
[0]->0 [1]->0 [2]->0 [3]->0 [4]->0 [5]->0 [6]->0 [7]->0
[8]->1 [9]->1 [10]->1 [11]->1 [12]->1 [13]->1 [14]->1 [15]->1
[16]->7 [17]->2 [18]->2 [19]->2 [20]->2 [21]->2 [22]->2 [23]->2
[24]->3 [25]->3 [26]->3 [27]->3 [28]->3 [29]->3 [30]->3 [31]->3
[32]->4 [33]->4 [34]->4 [35]->4 [36]->4 [37]->4 [38]->4 [39]->4
[40]->5 [41]->5 [42]->5 [43]->5 [44]->5 [45]->5 [46]->5 [47]->5
[48]->6 [49]->6 [50]->6 [51]->6 [52]->6 [53]->6 [54]->6 [55]->6
[56]->7 [57]->7 [58]->7 [59]->7 [60]->7 [61]->7 [62]->7 [63]->7
```

To verify the WGB QoS mapping statistics on Data Plane, run the **show datapath qos-mapping statistics** command.

```
Device# show datapath qos-mapping statistics

======= pkt stats per dscp-mapping rule =======
dscp up pkt_cnt
16 7 0
```

To clear the WGB QoS mapping statistics on Data Plane, run the **clear datapath qos-mapping statistics** command.

Note The command clears packet count statistics per rule on data-plane.

Packet Capture: TCP Dump on WGB

Packet Capture: TCP dump utilities

TCP dump utilities are network packet analyzers that

- captures packets transmitted over network interfaces,
- displays and saves packet data for monitoring and troubleshooting, and
- enables in-depth analysis of wired network traffic on WGBs.

TCP Dump on WGB chapter provides information on how to enable TCP dump through the WGB wired interface on the Catalyst IW9167EH .

Purpose of TCP dump utility

TCP dump on a WGB monitors and troubleshoots network communications, ensuring the WGB relays frames correctly between the wired clients and the wireless networks.

The TCP dump utility

- displays captured packets in real time on the WGB terminal, and
- capture packets to storage.

Note The TCP dump utility does not support the simultaneous capture of packets to storage and printing them on the WGB terminal.

Packet capture modes

The WGB packet capture utility supports the following modes and behaviors:

- Default: Displays captured packets with header in the real time on the WGB terminal
- Verbose: Parses and prints real-time packets on the WGB terminal, displaying the headers and prints the data of each packet, including its link-level header, in hexadecimal format.

Note Reformat the verbose output for text2pcap compatibility.

In default or verbose mode, the WGB terminal can print a maximum of 1000 packet entries.

- Capture: Captures packets to a file storage instead of printing them in real time. Use the **show pcap** command to view the captured internal wired packets.

Note Every round of Packet Capture (PCAP) clears the existing PCAP file.

Before any new PCAP session, transfer the current PCAP file to an external server to prevent it from being overwritten.

PCAP stops automatically when the PCAP file reaches a size of 100 MB.

Protocol packet capture capabilities

You can capture packets from an AP either using a default or custom filter through the WGB wired port and then upload them to an external server.

The default filter captures three main protocol packets such as IP, TCP, or UDP.

A custom filter captures specific packets that are relevant for troubleshooting specific issues or monitoring certain types of network activity.

You can use different protocol filters to capture packets for debugging. For instance, include the given protocols in your filter expression:

- Transmission Control Protocol, Internet Control Message Protocol (ICMP) and ICMPv6
- Profinet with IP proto 0x8892
- Address Resolution Protocol (ARP)
- Internet Group Management Protocol (IGMP)
- User Datagram Protocol

- Dynamic Host Configuration Protocol (DHCP) with port 67 or port 68 and DHCPv6 with port 546 or port 547
- Common Industrial Protocol (CIP) with TCP port 44818
- Domain Name System (DNS) with port 53
- Simple Network Management Protocol with port 161 or port 162.



Note The protocols listed represent only a portion of the PCAP capabilities.

Filter expressions for packet captures

The filter expression for a PCAP comprises at least one primitive. Primitives usually consist of qualifiers followed by an identifier. The identifier can be a name or a number.

There are three kinds of qualifiers.

- Type: Specifies the type of the identifier. The type can be a port, a host, a network, or a range of ports.

  For example: port 20

- Dir: Specifies that the capture is for only packets with a given transfer direction.

  For example: src x.x.x.x and port ftp-data or dst x.x.x.x and port ftp

- Proto: Limits the capture to a specific protocol.

  For example: tcp port 21.

The filter expressions can be combined using the logical operators AND, OR, and NOT to create more specific and complex filters.



Note When constructing filter expressions, it is important to understand the order of operations and use parentheses to group expressions when necessary to ensure the correct interpretation.

Enable Wired Packet Capture on WGB

Procedure

Step 1 To enable PCAP, choose one of the options given here:

a. PCAP using default filter:

Device#**debug traffic wired** [*0* | *1*] {**ip** | **tcp** | **udp**} [**verbose** | **capture**]

[0-1]: Specifies the wired interface number. If not selected, capture packets from all the wired interface.

This table lists examples of PCAP in default, verbose, and capture modes:

Mode	Example
Default: Captures IP protocol header packets.	Device#**debug traffic wired 1 ip** APXXXX.XXXX.XXXX#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet) 1 08:35:50.529851 IP 209.165.200.213 > 209.165.200.1: ICMP echo request, id 13721, seq 1, length 64 2 08:35:50.534813 IP 209.165.200.1 > 209.165.200.213: ICMP echo reply, id 13721, seq 1, length 64
Verbose: Captures detailed information of the UDP protocol packets.	Device#**debug traffic wired 1 udp verbose** APXXXX.XXXX.XXXX#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet) 1 08:25:59.696990 IP6 fe80::322c:712c:5787:f246.dhcpv6-client > ff02::1:2.dhcpv6-server: dhcp6 solicit 0x0000: 3333 0001 0002 fc58 9a16 e428 86dd 6001 0x0010: 7b92 006d 1101 fe80 0000 0000 0000 322c 0x0020: 712c 5787 f246 ff02 0000 0000 0000 0000 0x0030: 0000 0001 0002 0222 0223 006d 00a6 010c 0x0040: d064 0008 0002 ffff 0006 001e 0034 0011 0x0050: 0015 0016 0017 0018 001f 0038 0040 0043 0x0060: 0052 0053 005e 005f 0060 0001 000a 0003 0x0070: 0001 fc58 9a16 e428 0014 0000 0027 0013 0x0080: 0006 4150 4643 3538 0439 4131 3604 4534 0x0090: 3238 0000 0300 0c00 0000 0100 0000 0000 0x00a0: 0000 00
Capture: Writes TCP packet information to the PCAP file.	Device#**debug traffic wired 1 tcp capture** % Writing packets to "/pcap/APXXXX.XXXX.XXXX_capture.pcap0" APXXXX.XXXX.XXXX#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet)

b. PCAP using custom filter:

Note
Enable only one PCAP process at a time. Do not use unsupported characters like " ` $ ^ & | \ > < ? ; and ~ in the filter expressions.

Device#**debug traffic wired** [*0* | *1*] **filter** *expression* [**verbose** | **capture**]

This table lists examples of PCAP in default, verbose, and capture modes:

Mode	Example
Default: Captures IP protocol header packets.	Device#**debug traffic wired 0 filter icmp** APXXXX.XXXX.XXXX#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet) 1 10:38:59.948729 IP 209.165.200.213 > 209.165.200.1: ICMP echo request, id 16204, seq 1, length 64 2 10:38:59.954308 IP 209.165.200.1 > 209.165.200.213: ICMP echo reply, id 16204, seq 1, length 64

Mode	Example
Verbose: Captures detailed information of the UDP protocol packets.	Device#**debug traffic wired 1 filter icmp verbose** APXXXX.XXXX.XXXX##reading from file /dev/click_wired_log, link-type EN10MB (Ethernet) 17:13:30.706493 IP 209.165.200.213 > 209.165.200.1: ICMP echo request, id 986, seq 1, length 64 0x0000: fc58 9a17 afd4 f8e4 3b9d 7322 0800 4500 0x0010: 0054 57a0 4000 4001 889e c0a8 6cc8 c0a8 0x0020: 6c51 0800 940c 03da 0001 7f3d 5365 0000 0x0030: 0000 cea2 0000 0000 0000 1011 1213 1415 0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 0x0060: 3637 17:13:30.710567 IP 209.165.200.1 > 209.165.200.213: ICMP echo reply, id 986, seq 1, length 64 0x0000: f8e4 3b9d 7322 fc58 9a17 afd4 0800 4500 0x0010: 0054 9102 0000 4001 8f3c c0a8 6c51 c0a8 0x0020: 6cc8 0000 9c0c 03da 0001 7f3d 5365 0000 0x0030: 0000 cea2 0000 0000 0000 1011 1213 1415 0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 0x0060: 3637
Capture: Writes TCP packet information to the PCAP file.	Device#**ddebug traffic wired 1 filter icmp capture** % Writing packets to "/tmp/pcap/APXXXX.XXXX.XXXX_capture.pcap0" APXXXX.XXXX.XXXX#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet)

For more information on filter expressions, see *TCP dump pcap-filter* documentation.

c. PCAP in multiple vlan using custom filter:

Note
Some custom filters miss traffic in non-native VLANs. For example, the custom filter command **#debug traffic wired 0 filter icmp** fails to capture downlink ICMP traffic in non-native VLANs.

To capture downlink traffic in non-native VLANs, you have two options:

- Include the VLAN in the filter expression to capture bidirectional traffic of the wired client in a non-native VLAN

```
Device#debug traffic wired 0 filter "icmp or (vlan and icmp)"
1  12:27:40.833815 IP 209.165.200.102 > 209.165.200.1: ICMP echo request, id 27279, seq 1, length 64
2  12:27:40.841331 IP 209.165.200.1 > 209.165.200.102: ICMP echo reply, id 27279, seq 1, length 64
```

- To capture all IP traffic including native vlan and non-native vlan, use the default IP filter.

```
Device#debug traffic wired 0 ip
1  12:27:40.833815 IP 209.165.200.102 > 209.165.200.1: ICMP echo request, id 27279, seq 1, length 64
2  12:27:40.841331 IP 209.165.200.1 > 209.165.200.102: ICMP echo reply, id 27279, seq 1, length 64
```

To disable wired PCAP, see Disable Wired Packet Capture on WGB.

Step 2 To upload the packets to an external server, use the command given here:

Note

Before uploading the packets, complete the PCAP process and save the packets to file.

Use TFTP, SFTP, or SCP server to upload the PCAP file to an external server.

Device#**copy pcap APxxxx.xxxx.xxxx_capture.pcap0 <tftp|sftp>://A.B.C.D[/dir][/filename]**

copy pcap APxxxx.xxxx.xxxx_capture.pcap0 scp://username@A.B.C.D[:port]:/dir[/filename]

Example:

```
Device#copy pcap APXXXX.XXXX.XXXX_capture.pcap0 scp://iot@209.165.200.213:/capture/wgb_sniffer.pcap
copy ""/pcap/APXXXX.XXXX.XXXX_capture.pcap0"" to
"scp://iot@209.165.200.213:/capture/wgb_dhcp_sniffer_0_46_29.pcap" (Y/N)Y
iot@209.165.200.213 password:
APXXXX.XXXX.XXXX_capture.pcap0                 0%    0     0.0KB/s   --:-- ETA
APXXXX.XXXX.XXXX_capture.pcap0               100% 2530   916.5KB/s   00:00
```

Disable wired packet captures

Procedure

Step 1 Use the **no debug traffic wired** [*0-3*]{**ip** | **tcp** | **udp**}[**verbose** | **capture**] command to disable PCAP with the default filter.

```
Device# no debug traffic wired 1 ip verbose
```

Step 2 Use the **no debug traffic wired** [*0-3*]**filter** *expression* [**verbose** | **capture**] command to disable PCAP with the custom filter.

```
Device# no debug traffic wired 0 filter "icmp or (vlan and icmp)" capture
```

Note
You can also use the **no debug** or **undebug all** command to terminate the capture process.

Verify wired packet capture

- To verify the debug status, use the **show debug** command.

```
Device#show debug
traffic:
  wired tcp debugging is enabled
```

- To view the captured internal wired packets stored in the file, use the **show pcap** command.

Note After capturing packets to the file, use the **show pcap** command to view them.

```
Device#show pcap
reading from file /pcap/APXXXX.XXXX.XXXX_capture.pcap0, link-type EN10MB (Ethernet)
1  00:00:00.000000 IP 0.0.0.0 > 224.0.0.1: igmp query v2
```

```
2  09:41:48.903670 IP 209.165.200.189 > 209.165.200.1: ICMP echo request, id 29920, seq
 1, length 64
3  09:41:48.908927 IP 209.165.200.1 > 209.165.200.189: ICMP echo reply, id 29920, seq
1, length 64
4  09:41:49.904914 IP 209.165.200.102 > 209.165.200.1: ICMP echo request, id 29920, seq
 2, length 64
5  09:41:49.909009 IP 209.165.200.1 > 209.165.200.102: ICMP echo reply, id 29920, seq
2, length 64
```

- To filter and view the basic content of captured packets sequentially, run the **show pcap [filter** *expression***]** command.

```
Device#show pcap filter "src 209.165.200.189"
reading from file /pcap/APXXXX.XXXX.XXXX_capture.pcap0, link-type EN10MB (Ethernet)
 1  09:41:48.903670 IP 209.165.200.189 > 209.165.200.1: ICMP echo request, id 29920,
seq 1, length 64
 2  09:41:48.908927 IP 209.165.200.1 > 209.165.200.189: ICMP echo reply, id 29920, seq
 1, length 64
```

- To filter and view the detailed content of a specific packet, run the **show pcap [filter** *expression***][detail** *no***]** command.

```
Device#show pcap filter "src 209.165.200.189" detail 2
2024-04-25 09:41:49.904914
000000 18 59 f5 96 af 74 00 50 56 85 8a 0a 08 00 45 00
000010 00 54 14 6c 40 00 40 01 b7 9d 64 16 53 72 64 16
000020 53 01 08 00 70 81 74 e0 00 02 d4 3e 2b 66 00 00
000030 00 00 50 24 04 00 00 00 00 00 10 11 12 13 14 15
000040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
000050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
000060 36 37
```

AAA User Authentication Support

AAA user authentications

AAA user authentication is a network management mechanism that:

- controls access to network resources through user authentication,
- assigns differentiated privilege levels to users, and
- manages usernames and passwords centrally on the AAA server.

From Release 17.15.1, AAA-based user management and authentication are supported on IW9167EH WGB.

The AAA server assigns privilege levels (0–15) via Authorization-Reply messages. Only levels 1 (view user) and 15 (management user) are supported. Levels 2–14 are reserved and must not be assigned.

If a user is added without a privilege level, WGB will assign the lowest privilege level to that user.

Features of AAA-based user management and authentication

AAA-based user management and authentication includes these features:

- Provides multiple-user support
- Stores usernames and passwords on the AAA server

- Authenticates users with AAA
- Supports differentiated user privileges
- Restricts CLI access based on user privileges

Note Similar to a Cisco Router or Switch, the Workgroup Bridge (WGB) can also create and store usernames and passwords locally.

Configure AAA Server

Before you begin

- You can add a secondary AAA server (RADIUS or TACACS+) before adding a primary AAA server. Once the primary AAA server is added, clients connect to the primary AAA server.
- When both primary and secondary RADIUS servers are configured, the WGB attempts to connect with the primary RADIUS server three times before switching to the secondary RADIUS server.
- For the TACACS+ server, the connection attempt is done only once with the primary TACACS+ server. If the primary TACACS+ server fails to respond, the secondary TACACS+ server is used.

Note The WGB AAA RADIUS server configuration command is officially supported starting from the 17.15.1 release.

If you downgrade the image from release 17.15.1 or later to 17.14.1 or earlier, or upgrade from 17.14.1 or earlier to 17.15.1 or later, the configured RADIUS server port resets to zero. Reconfigure the RADIUS server port.

Procedure

Add or remove a AAA server (RADIUS or TACACS+).

Option	Description
Configure a AAA server	Use the **config** {**radius** | **tacplus**} **authentication** {**primary** | **secondary**}**add** {**ipv4** | **ipv6**}*ip-address* **port** *port-number* **secret** *secret-string* command. `Device# configure radius authentication primary add ipv4 10.10.10.5 port 100 secret radiusSecret123` **Note** Do not use unsupported characters in secret-string parameters. These characters include the vertical bar (|), semicolon (;), dollar sign ($), less than (<), greater than (>), ampersand (&), caret (^), grave accent (`), backslash (), carriage return (\r), and double quotation marks (“”).

Option	Description
Remove a AAA server	Use the **config** {**radius** | **tacplus**} **authentication** {**primary** | **secondary**} **delete** command. `Device# configure radius authentication primary delete`

Enable or disable RADIUS authentication for login user

Procedure

Step 1 Enable or disable AAA RADIUS authentication for the login user using one of the options.

Option	Description
Enable AAA RADIUS authentication for the login user	Use the **config ap management aaa radius enable** command. `Device# config ap management aaa radius enable`
Disable AAA RADIUS authentication for the login user	Use the **config ap management aaa radius disable** command. `Device# config ap management aaa radius disable`

Step 2 (Optional) Use the **show running-config | include aaa** command to verify the AAA server (RADIUS or TACACS+) configuration.

```
Device# show running-config | include aaa

AAA server configuration:-
==============================
Status: Enabled
AAA server type : radius
Primary RADIUS IP address : 192.0.2.0
Primary RADIUS port : 1812
.
.
.
```

Enable or disable TACACS+ authentication for login user

Procedure

Step 1 Enable or disable AAA RADIUS authentication for the login user using one of the options.

Option	Description
Enable AAA TACACS+ authentication for the login user	Use the **config ap management aaa tacplus enable** command. `Device# config ap management aaa tacplus enable`
Disable AAA TACACS+ authentication for the login user	Use the **config ap management aaa tacplus disable** command. `Device# config ap management aaa tacplus disable`

Step 2 (Optional) Use the **show running-config | include aaa** command to verify the AAA server (TACACS+) configuration.

```
Device# show running-config | include aaa

AAA server configuration:-
==============================
Status: Enabled
AAA server type : tacplus
Primary TACPLUS IP address : 192.0.2.0
Primary TACPLUS port : 49
.
.
.
```

AAA authentication configuration example

When AAA RADIUS authentication is enabled, using the show running-config command generates this sample output.

```
Device# show running-config

AAA server configuration:-
==============================
Status: Enabled
AAA server type : radius
Primary RADIUS IP address : 192.0.2.0
Primary RADIUS port : 1812
.
.
.
```

When AAA TACACS+ authentication is enabled, using the show running-config command generates this sample output.

```
Device# show running-config

AAA server configuration:-
==============================
Status: Enabled
AAA server type : tacplus
Primary TACPLUS IP address : 192.0.2.0
Primary TACPLUS port : 49
.
.
.
```

Port Address Translation

Port address translations

Port Address Translation (PAT), also known as Network Address and Port Translation (NAPT), is a network address translation method that:

- translates multiple internal wired client private IP addresses and port numbers
- to unique public IP addresses and port numbers
- before sending packets to the external network.

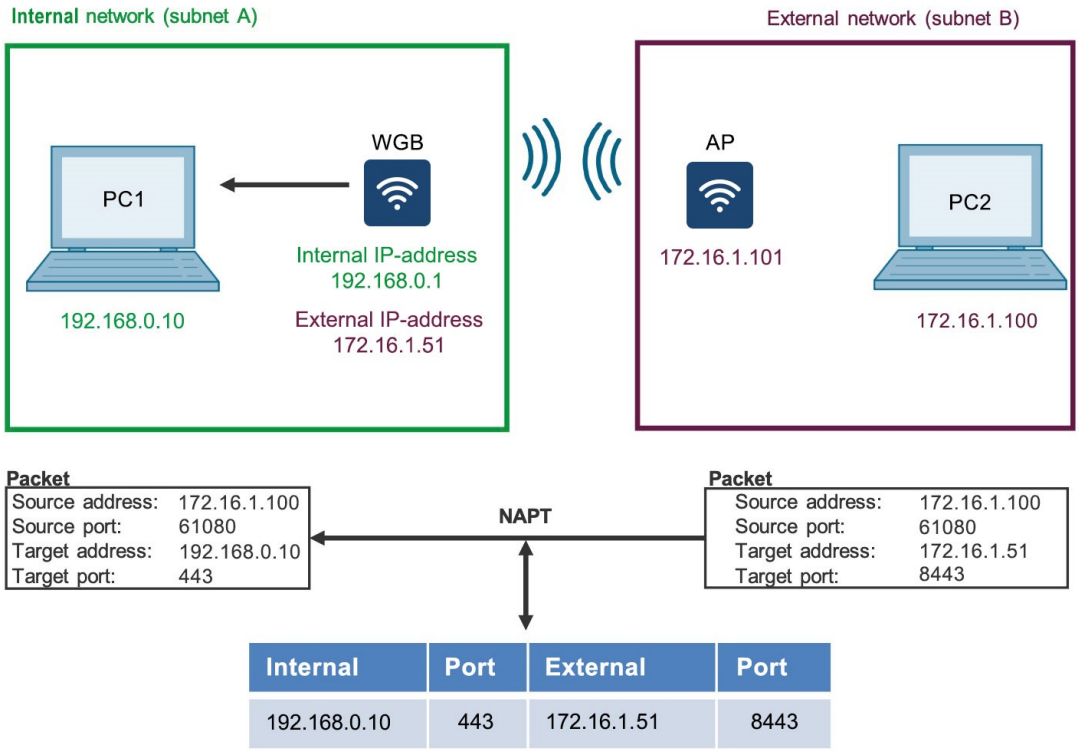
A private IP address is used only within an internal network. A public IP address is globally unique and used on the Internet. NAPT mapping uses both the IP address and the port number. This allows packets from multiple internal hosts to map to the same external IP address with different port numbers. This enables client devices within the internal local subnet to reuse the same IP addresses across different Automated Guided Vehicles (AGVs).

From UIW Release 17.16.1, PAT is supported on the IW9165E Workgroup Bridge (WGB) Access Points (APs) of each AGV.

Note Profinet clients on the AGV must be configured with a unique IP address that belongs to the global subnet.

This image illustrates the concept of Network Address Port Translation (NAPT), demonstrating how a Wireless Gateway Bridge (WGB) translates incoming packets from an external network to an internal host by mapping external IP addresses and ports to internal ones.

Figure 6: NAPT Translation Between Internal and External Networks



Supported protocol

NAPT supports TCP and UDP for communication between devices on the internal and external networks.

Limitations for WGB

- NAT is not supported for incoming packets with an 802.1Q VLAN tag behind the device.
- Multicast traffic is not supported for NAT inside wired clients.
- FTP traffic is supported in active mode. In passive mode, FTP traffic is supported only when the FTP server is located within the NAT inside.
- The TFTP protocol is supported only when the TFTP server resides inside the NAT.
- Application Layer Gateway (ALG) is not supported.

Limitations for uWGB

- Access Control Lists (ACLs) are not supported.
- The NAPT supports only one private LAN as the NAPT inside network.

NAPT rules and mapping tables

A NAPT rule and mapping table is a network translation mechanism that:

- defines how a Workgroup Bridge (WGB) translates internal private addresses and ports to an external, routable address and port,
- maintains a table that maps internal device traffic to corresponding global IP/port pairs, and
- supports both TCP and UDP protocols for address and port translation.

The configuration supports a maximum of 256 IP NAT rules on WGB.

NAPT mapping table

The mapping table is created and managed based on the traffic and NAPT rules.

NAPT uses entries containing the source IP address, source port number, protocol type, destination IP address, and destination port number (TCP or UDP). These entries enable the system to translate addresses, filter packets, and index the NAPT mapping table.



Note The maximum number of mapping entries in NAPT translation table is 4096.

This table shows an example of a NAPT mapping.

Table 4: NAPT Mapping Table

Protocol	Internal Local IP Address and Port	WGB Global IP Address	External Global IP Address and Port
TCP	192.168.0.10: 80	172.16.100.11	172.16.100.11: 61080

Upstream and downstream data flows

Upstream and downstream data flows are types of network traffic flows that:

- use Network Address and Port Translation (NAPT) to translate source or destination addresses,
- allow secure transfer of data between internal and external networks, and
- maintain privacy and integrity of IP addresses.

Downstream data flow using NAPT

Downstream data flow refers to the flow of data from the external network to the AGV's internal network. The gateway (WGB or uWGB) manages communication between the external and internal networks..

When packets arrive with an external IP address and port number, the mapping table is checked to identify the corresponding internal destination.

The packets are then translated and forwarded to the internal network based on the destination IP address and port number.

The diagram illustrates how address and port translation manages both upstream (internal-to-external) and downstream (external-to-internal) traffic flows between private LAN clients and external networks.

Figure 7: Upstream and downstream data flow using NAPT in WGB

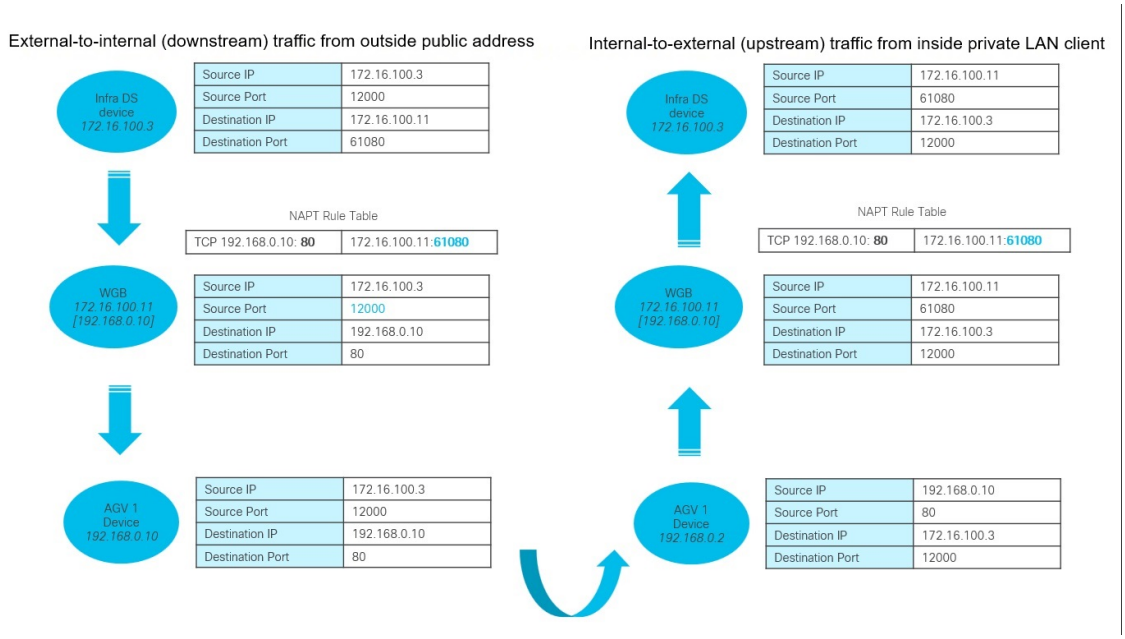
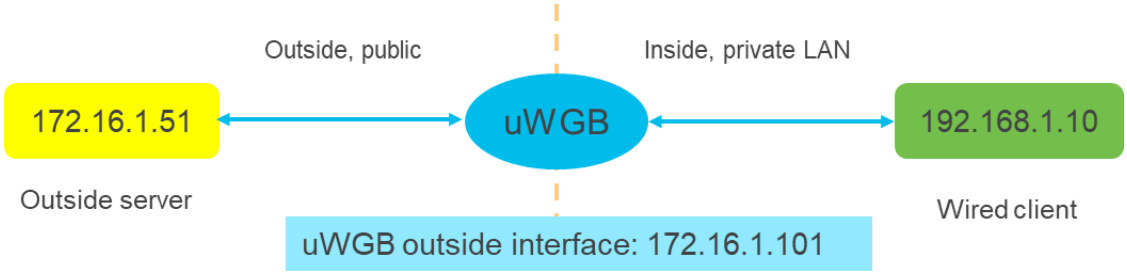


Figure 8: Upstream and downstream data flow using NAPT in uWGB



Upstream data flow using SNAT

Upstream data flow refers to the transfer of packets from internal networks to external networks. The gateway enables communication between the two networks.

All outgoing packets from the internal network are translated to the external network using Source Network Address Translation (SNAT).

For upstream traffic, SNAT replaces the source IP address and port numbers with the gateway's IP address, ensuring that internal IP addresses are not exposed to the external network.

Configure NAPT on WGB

This procedure describes how to configure Source Network Address Translation (SNAT) for upstream data flow and Network Address and Port Translation (NAPT) for downstream data flow.

Complete Steps 1 to 3 to configure upstream data flow using SNAT.

Complete Steps 4 and 5 to configure downstream data flow using NAPT.

Procedure

Step 1 Use the **configure ip nat enable** command to enable NAPT.

```
Device#configure ip nat enable
```

Use the **configure ip nat disable** command to disable the NAPT.

Step 2 Use the **configure ip nat address add ip** *inside- ip-address* **netmask** *netmask* command to configure inside IPv4 address and netmask.

```
Device# configure ip nat address add ip 192.168.0.1 netmask 255.255.255.0
```

Step 3 (Optional) Use the **configure ip nat inside port range** *min-port-number max-port-number* command to configure SNAT port range for upstream data flow.

```
Device# configure ip nat inside port range 32000 33000
```

The valid range is 1–65535. The default range is 30000–59999.

Note
Ensure that the SNAT port range and the NAPT port range do not overlap.

Step 4 Use the **configure ip nat outside port range** *min-port-number max-port-number* command to configure NAPT port range for downstream data flow.

```
Device# configure ip nat outside port range 34000 62000
```

The valid range for outside port numbers is 1025–65535. Do not use reserved ports 1233, 1234, or 20000.

Note
Ensure the NAPT and SNAT port ranges do not overlap.

Step 5 Use the **configure ip nat rule add inside ip** *inside-ip-address* **port** *inside-port-number* **outside port** *outside-port-number* **protocol** { **tcp** | **udp** } command to configure the NAPT mapping rule for downstream data flow.

```
Device#configure ip nat rule add inside ip 192.168.0.10 port 80 outside port 61080 protocol tcp
```

inside-ip-address is the internal wired client network IP address.

inside-port-number is the internal wired client network TCP or UDP port number.

Outside port number must be within the configured NAPT range.

Step 6 (Optional) Use the **show ip nat configuration** command to view the current NAPT configuration.

```
Device# show ip nat configuration

IP NAT Configuration are:
===================================
Status: enabled
```

```
inside interface ip/netmask: 192.168.0.1/255.255.255.0
SNAT port range: 10000 - 20000
NAPT port range: 61000 - 65535
The number of ip nat rules: 1
Id       Outside_port    Inside_ip          Inside_port    Protocol
0        61080           192.168.0.10       80             tcp
```

Step 7 (Optional) Use the **show ip nat tranlations** command to view the current NAPT translation entries from the NAPT rule table.

```
Device# show ip nat translations
UDP:
    src_ip    port    dst_ip    port    =>    src_ip    port    dst_ip    port   direction
expiry_time
(192.168.0.10, 41278, 172.16.1.51, 22000) => (172.16.1.101, 30004, 172.16.1.51, 22000) [forward] exp:
 290
(172.16.1.51, 22000, 172.16.1.101, 61080) => (172.16.1.51, 22000, 192.168.0.10, 41278) [reverse] exp:
 290
====================================
TCP:
    src_ip    port    dst_ip    port    =>    src_ip    port    dst_ip    port   direction
expiry_time
(192.168.0.10, 80, 172.16.100.3, 443) => (172.16.100.11, 30000, 172.16.100.3, 443) [forward] exp:
138
(172.16.100.3, 443, 172.16.100.11, 30000) => (172.16.100.3, 443, 192.168.0.10, 80) [reverse] exp:
138
```

In the output, 'forward' refers to the log details of data packets processed by the WGB, including the source, destination, and translation information.

'Reverse' refers to the log details of return traffic, ensuring that responses from the destination reach the original source by reversing the traffic direction. It ensures the response from the destination correctly reaches back to the source by reversing the direction of the original traffic.

Delete NAPT mapping rule

This procedure describes how to delete NAPT configuration entries. You can remove a specific NAPT mapping rule by specifying the inside and outside parameters. You can also delete a rule by its rule ID or clear all NAPT rules from the configuration. Choose the method based on whether you want to remove a specific rule or reset the entire NAPT configuration.

Procedure

Delete NAPT mapping rule using one of the options given here:

Option	Description
Delete a NAPT mapping rule	Use the **configure ip nat rule delete inside ip** *inside- ip-address* **port** *inside-port-number* **outside port** *outside-port-number* **protocol** {**tcp** | **udp**} command. `Device#configure ip nat rule delete inside ip 192.168.1.10 port 80 outside port 61080 protocol tcp`

Option	Description
Delete the NAPT mapping rule as per the rule-id	Use the **configure ip nat entry delete** *rule-id* command. `Device# configure ip nat entry del 0` **Note** You can use the **show ip nat configuration** command to view the rule-id.
Delete all the NAPT mapping rules	Use the **configure ip nat entry delete all** command. `Device# configure ip nat entry delete all`

Delete NAPT IP address

This procedure explains how to delete the configured NAT IP addresses. You can remove the gateway IPv4 address assigned to the internal wired client. Alternatively, you can delete the external IPv4 address configured on the NAT outside interface.

Note To remove all the NAPT configuration, you should also delete the IP address and interface.

Procedure

Delete the NAPT IP address using one of the options given here:

Option	Description
Delete gateway IPv4 address for the internal wired client	Use the **configure ip nat address delete** command. `Device#configure ip nat address delete`
Delete the external IPv4 address	Use the **configure interface nat-outside address delete** command. `Device#configure interface nat-outside address delete`

Verify NAPT on WGB

Verify NAPT configuration

Use the **show ip nat configuration** command to print the current NAPT configuration on WGB.

```
Device#show ip nat configuration
IP NAT Configuration are:
====================================
Status: enabled
inside interface ip/netmask: 192.168.0.1/255.255.255.0
```

```
SNAT port range: 10000 - 20000
NAPT port range: 61000 - 65535
The number of ip nat rules: 1
Id       Outside_port    Inside_ip          Inside_port    Protocol
0        61080           192.168.0.10       80             tcp
```

Verify NAPT entry

Use the **show ip nat tranlations** command to print the current NAPT translation entries from the NAPT rule table.

```
Device#show ip nat translations
UDP:
    src_ip    port    dst_ip    port    =>    src_ip    port    dst_ip    port   direction
    expiry_time
(192.168.0.10, 41278, 172.16.1.51, 22000) => (172.16.1.101, 30004, 172.16.1.51, 22000)
[forward] exp: 290
(172.16.1.51, 22000, 172.16.1.101, 61080) => (172.16.1.51, 22000, 192.168.0.10, 41278)
[reverse] exp: 290
====================================
TCP:
    src_ip    port    dst_ip    port    =>    src_ip    port    dst_ip    port   direction
    expiry_time
(192.168.0.10, 80, 172.16.100.3, 443) => (172.16.100.11, 30000, 172.16.100.3, 443) [forward]
 exp: 138
(172.16.100.3, 443, 172.16.100.11, 30000) => (172.16.100.3, 443, 192.168.0.10, 80) [reverse]
 exp: 138
```

In the output, forward refers to the log details of the WGB processed data packets, which include details such as source, destination and any translation performed.

Reverse refers to the log details of the return traffic based on the original packets forwarded by the WGB. It ensures the response from the destination correctly reaches back to the source by reversing the direction of the original traffic.

Port Address Translation on uWGB

Port Address Translation

From UIW Release 17.16.1, Port Address Translation (PAT) is supported on the IW9167EH uWGB of each Automated Guided Vehicle (AGV).

PAT, also known as Network Address and Port Translation (NAPT), translates multiple internal wired client private IP addresses and port numbers to unique public IP address and port numbers before sending the packets to the external network.

A private or internal IP address is used only in an internal network, whereas a public or external IP address is used on the Internet and is globally unique.

NAPT mapping is based on the IP address and the port number. With NAPT, packets from multiple internal hosts are mapped to the same external IP address with different port numbers.

Client devices within the internal local subnet can reuse the same IP addresses across different AGVs.

Precondition

In a NAPT deployment, AGV devices in the internal local subnet have pre-configured IP address.

Supported protocol

NAPT supports TCP or UDP to communicate between devices on the internal and external network.

Limitation of NAPT

The NAPT limitations are:

- The NAPT does not support Access Control Lists (ACLs).
- The NAPT supports only one private LAN as the NAPT inside network.

NAPT rule and mapping table

NAPT rule

The uWGB creates the default mapping rule based on the configured IP addresses, and it translates traffic flow triggered by internal client devices.

Configure a NAPT mapping rule to manage translation for traffic coming from external hosts.

The default mapping rule consists of `<inside-IP-address, inside-tcp-or-udp-port>, <outside-ip-address, predefined port range>, and <protocol>`, where the protocol can be either UDP or TCP.

NAPT mapping table

The uWGB creates and manages the mapping table based on the traffic and NAPT rules.

NAPT uses flow identifiers such as source address, source port, destination address, destination port, and IP protocol (TCP or UDP) to index the NAPT mapping table.

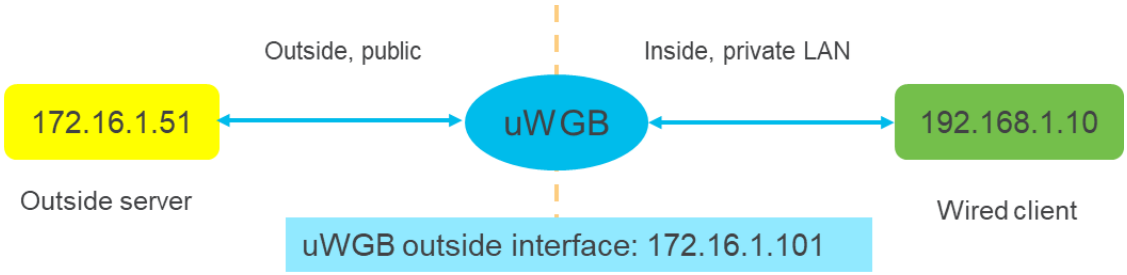
Note The maximum number of mapping entries in NAPT translation table is 4096, and these entries automatically appear in pairs.

Table 5: NAPT Mapping Table

Protocol	Inside Local IP Address and Port	uWGB Global IP Address	Outside Global IP Address and Port
TCP	192.168.1.10: 80	172.16.1.101	172.16.1.101: 61080

Upstream and downstream data flow

Figure 9: Upstream and downstream Data Flow Using NAPT



Upstream data flow using SNAT

Upstream data flow refers to the flow of packets from the internal networks to the external networks. The uWGB acts as a gateway between the internal and external networks. The uWGB translates all outgoing packets from the internal network to the external network using Source Network Address Translation (SNAT).

The SNAT translates the source IP address of the packets passing through the uWGB replacing it with the uWGB client IP address. This ensures that internal IP address are not exposed to the external network.

Downstream data flow using NAPT

Downstream data flow refers to the flow of data from the external network to the AGV's internal network. The uWGB acts as a gateway between the external and internal networks.

When the uWGB receives the packets with the external IP address and port, uWGB checks the mapping table to match the destination IP address and the destination TCP or UDP port of the incoming packet.

If the rule matches, uWGB translates the destination IP address and port numbers according to the matched entry in the table and forwards the packets to the internal network.

Configure NAPT on uWGB

This procedure describes how to configure Source Network Address Translation (SNAT) for upstream data flow and Network Address and Port Translation (NAPT) for downstream data flow.

Follow Step 1 through Step 4 to configure support for upstream data flow using SNAT.

Follow Step 5 and Step 6 to to configure support for downstream data flow using NAPT.

Procedure

Step 1 Use the **configure ip nat enable** command to enable NAPT.

```
Device#configure ip nat enable
```

Note
Use the **configure ip nat disable** command to disable the NAPT.

Step 2 (Optional) Use the **configure ip nat inside port range** *min-port-number max-port-number* command to configure SNAT port range for upstream data flow.

```
Device# configure ip nat inside port range 32000 33000
```

The valid range is 1025–65535. The default range is 30000–59999.

Note
The SNAT port range is the source port that the uWGB uses when sending traffic from internal network to the external network.

Ensure that the SNAT port range and the NAPT port range do not overlap.

Step 3 Use the **configure ip nat address add ip** *inside- ip-address* **netmask** *netmask* command to configure the gateway IPv4 address for the internal wired client on the uWGB.

```
Device# configure ip nat address add ip 192.168.0.1 netmask 255.255.255.0
```

Step 4 Use the **configure interface nat-outside address ipv4 static** *static-ip-address static-netmask gateway-ip-address* command to configure external IPv4 address on the uWGB.

```
Device# configure interface nat-outside address ipv4 static 172.16.1.101 255.255.255.0 172.16.1.1
```

static-ip-address is the uWGB own public address

gateway-ip-address is the uWGB external IP address.

The outside port number is automatically generated for upstream data flow.

The configuration supports the internal-to-external traffic flow.

Step 5 Use the **configure ip nat outside port range** *min-port-number max-port-number* command to configure NAPT port range on the uWGB to receive traffic from the external network to the internal network.

```
Device# configure ip nat outside port range 34000 62000
```

The valid range for outside port numbers is 1025–65535. Do not use reserved ports 1233, 1234, or 20000.

Note
Ensure the NAPT and SNAT port ranges do not overlap.

Step 6 Use the **configure ip nat rule add inside ip** *inside-ip-address* **port** *inside-port-number* **outside port** *outside-port-number* **protocol** {**tcp** | **udp**} command to configure the NAPT mapping rule for downstream data flow.

```
Device#configure ip nat rule add inside ip 192.168.0.10 port 80 outside port 61080 protocol tcp
```

inside-ip-address is the internal wired client network IP address.

inside-port-number is the internal wired client network TCP or UDP port number.

Outside port number must be within the configured NAPT range.

Step 7 (Optional) Use the **show ip nat configuration** command to view the current NAPT configuration.

```
Device# show ip nat configuration

IP NAT Configuration are:
====================================
Status: enabled
inside interface ip/netmask: 192.168.1.1/255.255.255.0
SNAT port range: 30000 - 59999
NAPT port range: 60000 - 65000
outside proxy ip/netmask/gateway: 172.16.1.101/255.255.255.0/172.16.1.1
The number of ip nat rules: 2
```

```
Id       Outside_port    Inside_ip          Inside_port    Protocol
0        61001           192.168.1.10       20001          udp
1        61002           192.168.1.10       20002          tcp
```

Step 8 (Optional) Use the **show ip nat tranlations** command to view the current NAPT translation entries from the NAPT rule table.

```
Device#show ip nat translations

ICMP:
    src_ip    dst_ip    port     =>       src_ip    dst_ip    port      direction    expiry_time
(172.16.1.1, 172.16.1.101, 30257) => (172.16.1.1, 192.168.1.10, 267) [reverse] exp: 272
(192.168.1.10, 172.16.1.1, 11) => (172.16.1.101, 172.16.1.1, 30001) [forward] exp: 272
====================================
UDP:
    src_ip    port    dst_ip    port    =>    src_ip    port    dst_ip    port   direction
expiry_time
(192.168.1.10, 20000, 172.16.1.51, 35200) => (172.16.1.101, 61001, 172.16.1.51, 35200) [reverse] exp:
 214
(192.168.1.10, 51184, 172.16.1.51, 22000) => (172.16.1.101, 30001, 172.16.1.51, 22000) [forward] exp:
 161
(172.16.1.51, 35200, 172.16.1.101, 61001) => (172.16.1.51, 35200, 192.168.1.10, 20000) [forward] exp:
 214
(172.16.1.51, 22000, 172.16.1.101, 30001) => (172.16.1.51, 22000, 192.168.1.10, 51184) [reverse] exp:
 161
====================================
TCP:
    src_ip    port    dst_ip    port    =>    src_ip    port    dst_ip    port   direction
expiry_time
(192.168.1.10, 44155, 172.16.1.51, 23000) => (172.16.1.101, 30002, 172.16.1.51, 23000) [forward] exp:
 238
(172.16.1.51, 23000, 172.16.1.101, 30002) => (172.16.1.51, 23000, 192.168.1.10, 44155) [reverse] exp:
 238
====================================
```

In the output, 'forward' refers to the log details of data packets processed by the uWGB, including the source, destination, and translation information.

'Reverse' refers to the log details of return traffic, ensuring that responses from the destination reach the original source by reversing the traffic direction. It ensures the response from the destination correctly reaches back to the source by reversing the direction of the original traffic.

Delete NAPT mapping rule

Follow this procedure to delete the NAPT mapping rule on the uWGB.

Procedure

Delete the configuration using the given commands as required.

- Use the **config ip nat rule delete inside ip** *inside- ip-address* **port** *inside-port-number* **outside port** *outside-port-number* **protocol** {**tcp** | **udp**} command to delete the NAPT mapping rule.

  ```
  Device#config ip nat rule delete inside ip 192.168.1.10 port 80 outside port 61080 protocol tcp
  ```

- Use the **configure ip nat entry delete** *rule-id* command to delete the NAPT mapping rule as per the rule-id.

```
Device#configure ip nat entry del 0
```

Note
Use the **show ip nat configuration** command to view the rule-id.

- Use the **configure ip nat entry delete** *all* command to delete all the NAPT mapping rules on the uWGB.

```
Device#configure ip nat entry delete all
```

Delete NAPT IP address

Follow this procedure to delete NAPT function IP address on the uWGB.



Note To completely remove the NAPT configuration, ensure to delete the IP address and the interface.

Procedure

Delete the necessary IP address of the NAPT function using the given commands as required.

- Use the **config ip nat address delete** command to delete the internal IPv4 address.

```
Device#Device#config ip nat address delete
```

- Use the **configure interface nat-outside address delete** command to delete the external IPv4 address.

```
Device#configure interface nat-outside address delete
```

Manage uWGB in NAPT deployment

Follow this procedure to manage uWGB in a NAPT deployment.

Before you begin

Ensure that all uWGB wired clients are in the private LAN.

Procedure

Step 1 Use the **configure dot11Radio 1 mode uwgb** *mac_address* **ssid-profile** *test_ssid* command to configure radio mode to uWGB.

```
Device# configure dot11Radio 1 mode uwgb FC:58:9A:17:0D:52 ssid-profile testssid
```

You can choose any unique MAC address, or use the optional method given below to calculate a unique MAC address.

Note
Ensure that the MAC address does not conflict with existing devices on the network to prevent connectivity issues.

To calculate the unique MAC address, add the offset value 0x12 to the base MAC address.

To find the base MAC address, use the **show controllers dot11Radio** *interface* command, as shown in Step 2.

Use the formula: base MAC address + offset = unique MAC address.

Note
Verify that the offset value is 0x12 or greater. For example, adding 0x12 to FC:58:9A:17:0D:40 results in FC:58:9A:17:0D:52.

Step 2 (Optional) Use the **show controllers dot11Radio 1** command to find the base MAC address.

```
Device#show controllers dot11Radio 1
wifi1     Link encap:Ethernet  HWaddr FC:58:9A:17:0D:40
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9109 errors:70 dropped:59043 overruns:0 frame:0
          TX packets:27920 errors:13 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:2699
          RX bytes:913806 (892.3 KiB)  TX bytes:5399794 (5.1 MiB)
```

Step 3 (Optional) Use the **show wgb dot11 associations** command to verify the uWGB is in the WGB state.

```
Device#show wgb dot11 associations
Uplink Radio ID            : 1
Uplink Radio MAC           : FC:58:9A:17:0D:52
SSID Name                  : SSID_NAME
Connected Duration         : 56 hours, 37 minutes, 11 seconds
Parent AP MAC              : B0:B8:67:3D:5E:D6
Uplink State               : CONNECTED
Auth Type                  : PSK
Key management Type        : WPA2
Uclient mac                : FC:58:9A:17:0D:52
Current state              : WGB
Uclient timeout            : 60 Sec
Dot11 type                 : 11ac
Channel                    : 157
Bandwidth                  : 20 MHz
Current Datarate (Tx/Rx)   : 156/144 Mbps
Max Datarate               : 156 Mbps
RSSI                       : 35
IP                         : 172.16.1.101/24
Default Gateway            : 172.16.1.1
IPV6                       : ::/128
Assoc timeout              : 100 Msec
Auth timeout               : 100 Msec
Dhcp timeout               : 60 Sec'
```

Step 4 Configure NAPT to enable end-to-end traffic flow for uWGB wired clients.

Verify NAPT on uWGB

Verify NAPT configuration

Use the **show ip nat configuration** command to print the current NAPT configuration on uWGB.

```
Device#show ip nat configuration

IP NAT Configuration are:
===================================
Status: enabled
inside interface ip/netmask: 192.168.1.1/255.255.255.0
SNAT port range: 30000 - 59999
NAPT port range: 60000 - 65000
outside proxy ip/netmask/gateway: 172.16.1.101/255.255.255.0/172.16.1.1
The number of ip nat rules: 2
Id       Outside_port    Inside_ip          Inside_port    Protocol
0        61001           192.168.1.10       20001          udp
1        61002           192.168.1.10       20002          tcp
```

Verify NAPT entry

Use the **show ip nat tranlations** command to print the current NAPT translation entries from the NAPT rule table.

```
Device#show ip nat translations
ICMP:
    src_ip    dst_ip    port     =>       src_ip    dst_ip    port      direction
expiry_time
(172.16.1.1, 172.16.1.101, 30257) => (172.16.1.1, 192.168.1.10, 267) [reverse] exp: 272
(192.168.1.10, 172.16.1.1, 11) => (172.16.1.101, 172.16.1.1, 30001) [forward] exp: 272
===================================
UDP:
    src_ip    port    dst_ip    port    =>    src_ip    port    dst_ip    port   direction
    expiry_time
(192.168.1.10, 20000, 172.16.1.51, 35200) => (172.16.1.101, 61001, 172.16.1.51, 35200)
[reverse] exp: 214
(192.168.1.10, 51184, 172.16.1.51, 22000) => (172.16.1.101, 30001, 172.16.1.51, 22000)
[forward] exp: 161
(172.16.1.51, 35200, 172.16.1.101, 61001) => (172.16.1.51, 35200, 192.168.1.10, 20000)
[forward] exp: 214
(172.16.1.51, 22000, 172.16.1.101, 30001) => (172.16.1.51, 22000, 192.168.1.10, 51184)
[reverse] exp: 161
===================================
TCP:
    src_ip    port    dst_ip    port    =>    src_ip    port    dst_ip    port   direction
    expiry_time
(192.168.1.10, 44155, 172.16.1.51, 23000) => (172.16.1.101, 30002, 172.16.1.51, 23000)
[forward] exp: 238
(172.16.1.51, 23000, 172.16.1.101, 30002) => (172.16.1.51, 23000, 192.168.1.10, 44155)
[reverse] exp: 238
===================================
```

In the output, forward means an entry from an actual traffic stream that uWGB processes and forwards. It logs the details of the packets translated and sent through the uWGB.

Reverse means an entry by reversing the direction of an existing forward. It records the expected return path or response for the traffic originally forwarded.

10 Mbps Speed Port Support on Cisco IW9167EH WGB

10 Mbps speed negotiation on Ethernet port

Earlier than Cisco IOS XE Release 17.16.1, the IW9167EH WGB does not support 10 Mbps speed on its ethernet ports. However, some clients still use devices with 10 Mbps Ethernet port. To enable compactibility with these devices.

Starting from Cisco IOS XE Release 17.16.1, the IW9167EH WGB supports 10 Mbps speed negotiation on the wired 0 port. This document explains how to enable and disable 10 Mbps speed negotiation on the WGB wired 0 port.

The WGB wired 0 port connects wired devices to the WGB, bridging wired and wireless network segments.

Speed negotiation

Speed negotiation, or auto-negotiation, is a process where two connected Ethernet devices automatically choose the best common transmission parameters, like speed and duplex mode, to optimize communication.

Speed and duplex are auto-negotiated based on the capabilities of the locally connected endpoint.

Note Disable the 10 Mbps feature when you connect devices that support 100 Mbps and 1 Gbps.

Benefits

This feature allows you to connect your 10 Mbps Ethernet devices to the IW9167EH WGB APs without replacing them.

Enable 10 Mbps speed port on Cisco IW9167EH WGB

Use this task to enable the 10 Mbps speed on the Ethernet port. You can execute the **show** commands as needed and do not have to follow a specific sequence.

Procedure

Step 1 Use the **enable** command to enable privileged EXEC mode.

```
Device>enable
```

Step 2 Use the **configure wired** *wired-port-number* **speed** *port-speed* **enable** command to enable 10 Mbps speed capability on the wired 0 port.

```
Device#configure wired 0 speed 10 enable
```

Step 3 (Optional) Use the **show running-config** command to verify 10 Mbps speed port status on the wired 0 port.

```
Device#show running-config
feature 10M speed
```

```
Interface wired0 10Mbps Configuration:
==================================
Status: Enable
```

Step 4 Use the **show ip interface brief** command to verify speed negotiation on the wired 0 port.

```
Device#show ip interface brief
Interface            IP-Address      Method   Status   Protocol   Speed      Duplex
*wired0              unassigned      unset    up       up         10         full
wired1               n/a             n/a      down     down       n/a        n/a
auxiliary-client     192.168.163.91  static   up       up         n/a        n/a
wifi0                n/a             n/a      down     down       n/a        n/a
wifi1                n/a             n/a      up       up         n/a        n/a
wifi2                n/a             n/a      up       up         n/a        n/a
```

Disable 10 Mbps speed port on Cisco IW9167EH WGB

Use this task to disable the 10 Mbps speed on the Ethernet port. You can execute the **show** commands as needed and do not have to follow a specific sequence.

Procedure

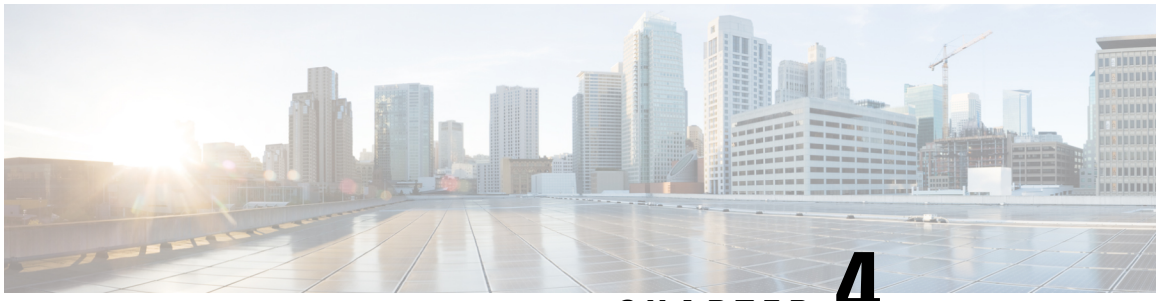
Step 1 Use the **configure wired** *wired-port-number* **speed** *port-speed* **disable** command to disable 10 Mbps speed capability on the wired 0 port.

```
Device# configure wired 0 speed 10 disable
```

Step 2 (Optional) Use the **show running-config** command to verify 10 Mbps Speed Port Status on the wired 0 port.

```
Device#show running-config
feature 10M speed

Interface wired0 10Mbps Configuration:
==================================
Status: Disable
```



CHAPTER 4

Automated Frequency Coordination

- AFC Support for 6 GHz Standard Power Mode , on page 107
- Verifying AFC Status on AP, on page 108

AFC Support for 6 GHz Standard Power Mode

The Cisco Catalyst IW9167EH access point has eight N-type female connectors to support multiple antenna options, such as the Self-Identifying Antennas (SIA) on designated three SIA ports, dual-band antennas, and single-band antennas. The IW9167EH is compatible with SIA antennas for the 6 GHz band.

The IW9167EH supports the Automated Frequency Coordination (AFC) 6 GHz Standard Power mode. A standard power AP joins the system. Before enabling standard power, the AP must get the available frequencies and the power in each frequency range from the AFC system.

The AFC system computes the available frequencies and maximum allowable power based on the information provided by the regulatory body (FCC for United States). The response is sent back to controller, which may assign a standard power channel to the AP based on the allowed channel list returned by the AFC system.

Standard Power AP coordinate through an AFC service. The AFC accesses information and, along with the AP's geographical location and antenna characteristics, creates a topographical propagation map modeling the AP's interference radius. This map allows you to assign maximum transmission power and coordinate/configure the channel settings to avoid interference.

Note A power cycle is mandatory after the first installation of the SIA antenna.

Table 6: Radio 6 GHz power mode support

Deployment Mode	Low Power Indoor Support	Standard Power Support
Outdoor	No	Yes

The transmission power is limited to a maximum of 36 dBm Effective Isotropic Radiated Power (EIRP), and APs must be coordinated through an AFC service. In the U.S., APs are allowed to operate in the UNII-5 frequency band from 5.925 GHz to 6.425 GHz and the UNII-7 frequency band from 6.525 GHz to 6.875 GHz.

Table 7: 6 GHz Target Power

Antenna Gain	Max Conducted per Path Power (SP/AFC)		Tx x Rx Chains	Max EIRP (SP/AFC)
	20-80 MHz	160 MHz		
7 dBi	17 dBm	17 dBm	4x4	30 dBm

Verifying AFC Status on AP

To verify the AFC request and response data on AP, run the **show rrm afc** command.

```
Device#show rrm afc
Location Type: 1
Deployment Type: 2
Height: 129
Uncertainty: 5
Height Type: 0
Request Status: 5
Request Status Timestamp: 2023-08-31T06:20:17Z
Request Id Sent: 5546388983266789933
Ellipse 1: longitude: -121.935066 latitude: 37.512830 major axis: 43 minor axis:
 9 orientation: 36.818100
AFC Response Request ID: 5546388983266789933
AFC Response Ruleset ID: US_47_CFR_PART_15_SUBPART_E
```

To verify the current operating power mode, run the **show controllers dot11Radio 2 | i Radio** command.

```
Device#show controllers dot11Radio 2 | i Radio
Dot11Radio2     Link encap:Ethernet  HWaddr 24:16:1B:F8:06:C0
Radio Info Summary:
Radio: 6.0GHz (SP)
```

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2025 Cisco Systems, Inc. All rights reserved.